SPCSS
Státní pokladna
Centrum sdílených služeb

SMLOUVA O POSKYTOVÁNÍ SLUŽEB

evidovaná u Objednatele pod č. 9166/2024-NBÚ/80, S86/24

evidovaná u Poskytovatele pod č. SML2024115, č. j. SPCSS-05721/2024

Smluvní strany:

Státní pokladna Centrum sdílených služeb, s. p.

se sídlem:	Na Vápence 915/14, 130 00 Praha 3
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 76922	
zastoupený:	Mgr. Jakub Richter, 1. zástupce generálního ředitele
IČO:	03630919
DIČ:	CZ03630919
ID datové schránky:	ag5uunk
bankovní spojení:	Česká spořitelna, a. s.
číslo účtu:	6303942/0800

(dále jen „***Poskytovatel***" nebo také „***SPCSS***")

a

Česká republika – Národní bezpečnostní úřad

se sídlem:	Na Popelce 2/16, 150 06 Praha 5
zastoupená:	Mgr. Jan Čuřín, ředitel
IČO:	68403569
DIČ:	CZ68403569
ID datové schránky:	h93aayw
Bankovní spojení:	Česká národní banka
Číslo účtu:	105881/0710

(dále jen „***Objednatel***" nebo také „***NBÚ***")

(Objednatel a Poskytovatel dále jednotlivě též jen „***Smluvní strana***" nebo společně „***Smluvní strany***")

uzavírají v souladu s ustanovením § 1746 odst. 2 zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „***OZ***") tuto

Smlouvu o poskytování služeb

(dále jen „***Smlouva***")

OBSAH

I. ÚVODNÍ USTANOVENÍ

1.1 Objednatel prohlašuje, že:

1.1.1 je ústředním správním úřadem pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti;

1.1.2 není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „***Zákon o střetu zájmů***") (člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády) nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti;

1.1.3 splňuje veškeré podmínky a požadavky ve Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené;

1.1.4 ke dni uzavření Smlouvy vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů;

1.1.5 ve smyslu čl. 2 odst. 2 Nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny (dále jen „***Nařízení č. 269/2014***"), není fyzickou nebo právnickou osobou, subjektem či orgánem nebo fyzickou nebo právnickou osobou, subjektem či orgánem s nimi spojeným uvedeným v příloze I Nařízení č. 269/2014. Pokud v průběhu účinnosti Smlouvy dojde k nedodržení podmínky dle věty první tohoto pododstavce, zavazuje se Objednatel bezodkladně o této skutečnosti písemně informovat Poskytovatele;

1.2 Poskytovatel prohlašuje, že:

1.2.1 je státním podnikem dle zákona č. 77/1997 Sb., o státním podniku, ve znění pozdějších předpisů;

1.2.2 není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. C) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (dále jen „***Zákon o střetu zájmů***") (člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády) nebo jím ovládaná osoba vlastní podíl představující alespoň 25 % účasti společníka v obchodní společnosti;

1.2.3 splňuje veškeré podmínky a požadavky ve Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené;

1.2.4 ke dni uzavření Smlouvy vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů, a zároveň se zavazuje Objednatele o všech skutečnostech o hrozícím úpadku bezodkladně informovat;

1.2.5 je odborně způsobilý ke splnění všech jeho závazků podle Smlouvy;

1.2.6 se detailně seznámil s rozsahem a povahou předmětu plnění, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k realizaci předmětu plnění, a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění za dohodnuté maximální smluvní ceny uvedené ve Smlouvě; a

1.2.7 jím poskytované plnění odpovídá všem požadavkům vyplývajícím z platných právních předpisů, které se na plnění vztahují;

1.2.8 v souladu s varováním Národního úřadu pro kybernetickou a informační bezpečnost vydaným podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, ze dne 21. 3. 2022, sp. zn. 350–401/2022, č. j. 3381/2022-NÚKIB-E/350 (dále jen „***Varování NÚKIB***"), nemá významný vztah k Ruské federaci, tj.:

- nemá sídlo v Ruské federaci;
- není závislý na dodávkách z území Ruské federace;
- jeho významní dodavatelé ve smyslu § 2 písm. n) VoKB nepoužívají ICT služby či produkty závislé na dodavatelích s významným vztahem k Ruské federaci.

1.2.9 v souladu s čl. 5k Nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, není:

1.2.9.1 ruským státním příslušníkem, fyzickou či právnickou osobou nebo subjektem či orgánem se sídlem v Rusku,

1.2.9.2 právnickou osobou, subjektem nebo orgánem, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v bodě 1.2.9.1 tohoto pododstavce, nebo

1.2.9.3 fyzickou nebo právnickou osobou, subjektem nebo orgánem, které jednají jménem nebo na pokyn některého ze subjektů uvedených v bodě 1.2.9.1 nebo 1.2.9.2 tohoto pododstavce,

1.2.10 ve smyslu čl. 2 odst. 2 Nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny (dále jen „***Nařízení č. 269/2014***"), není fyzickou nebo právnickou osobou, subjektem či orgánem nebo fyzickou nebo právnickou osobou, subjektem či orgánem s nimi spojeným uvedeným v příloze I Nařízení č. 269/2014. Pokud v průběhu účinnosti Smlouvy dojde k nedodržení podmínky dle věty první tohoto pododstavce, zavazuje se Poskytovatel bezodkladně o této skutečnosti písemně informovat Objednatele,

1.2.11 ve smyslu varování Národního úřadu pro kybernetickou a informační bezpečnost, vydaného podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, ze dne 8. 3. 2023, sp. zn. 350–303/2023, č. j. 2236/2023-NÚKIB-E/350 (dále jen „***Varování II***") nemá nainstalován a nepoužívá aplikaci TikTok na zařízeních přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům;

1.2.12 bude nejpozději k 1. lednu 2025 zapsán v katalogu cloud computingu vedeného Digitální informační agenturou jako poskytovatel cloudových služeb bezpečnostní úrovně č. 4, a to v souladu s vyhláškou č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

1.3 Smluvní strany níže svým podpisem stvrzují, že v průběhu vyjednávání o této Smlouvě vždy jednaly čestně a transparentně a současně se zavazují, že takto budou jednat i při plnění této Smlouvy, a to po celou dobu její účinnosti.

1.4 Každá ze Smluvních stran prohlašuje:

1.4.1 že se nepodílí a ani v minulosti nepodílela na páchání trestné činnosti v jakékoli formě ve smyslu zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, v platném znění (dále jen „***ZTOPO***"),

1.4.2 že zavedla potřebná opatření, aby nedošlo ke spáchání trestného činu v jakékoli formě, který by jí mohl být přičten podle ZTOPO,

1.4.3 že zavedla náležitá kontrolní a jiná obdobná opatření nad činností svých zaměstnanců, aby nevznikla trestní odpovědnost fyzických osob podle zákona č. 40/2009 Sb., trestní zákoník,

1.4.4 že učinila nezbytná opatření k zamezení nebo odvrácení případných následků spáchaného trestného činu,

1.4.5 že z hlediska prevence trestní odpovědnosti právnických osob učinila vše, co po ní lze spravedlivě požadovat, např. přijala Etický kodex a zásady Compliance programu.

1.5 Každá ze Smluvních stran prohlašuje, že nebude tolerovat jednání, které by mohlo naplňovat skutkové podstaty korupčních trestných činů, zejména trestných činů přijetí úplatku, nepřímého úplatkářství, podplácení a legalizace výnosů z trestné činnosti, přičemž důvodné podezření ohledně možného naplnění skutkové podstaty těchto trestných činů je příslušná Smluvní strana povinna neprodleně oznámit druhé Smluvní straně bez ohledu a nad rámec splnění případné zákonné oznamovací povinnosti.

1.6 V této souvislosti se Smluvní strany zavazují si navzájem neprodleně oznámit důvodné podezření ohledně možného jednání, které je v rozporu se zásadami podle tohoto článku a mohlo by souviset s plněním této Smlouvy nebo s jejím uzavíráním.

1.7 Smluvní strany prohlašují, že jsou jim známy zásady, hodnoty a cíle druhé Smluvní strany a zavazují se v co nejširším možném rozsahu (pokud to povaha jednotlivých ustanovení umožňuje) tyto zásady a hodnoty dodržovat, a to na vlastní náklady a odpovědnost při plnění svých závazků vzniklých z této Smlouvy.

1.8 Pojmy s velkými počátečními písmeny definované ve Smlouvě budou mít význam, jenž je jim ve Smlouvě, včetně jejích příloh a dodatků, připisován.

1.9 Smluvní strany souhlasí s tím, že označování dokumentů vzniklých na základě této Smlouvy bude ze strany Poskytovatele probíhat v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.first.org/tlp/).

II. ÚČEL SMLOUVY

2.1 Základním účelem, pro který se Smlouva uzavírá, je zajištění, zprovoznění a poskytnutí infrastruktury PaaS (platform as a sevice) Portálu úplného elektronického podání (dále jen „***PÚEP***“) pro IS Cefeus. Služba musí splňovat 4. (tj. kritickou) bezpečnostní úroveň cloud computingu z důvodu ochrany osobních údajů žadatelů o bezpečnostní prověrky. Veškeré ve Smlouvě a jejích přílohách uvedené požadavky na poskytování služeb musí být primárně vykládány tak, aby Objednatel realizací předmětu Smlouvy Poskytovatelem dosáhl zde uvedeného účelu.

III.PŘEDMĚT SMLOUVY

3.1 Předmětem této Smlouvy je úprava vzájemných práv a povinností Smluvních stran pro účely poskytování Služby dle specifikace uvedené níže v tomto článku.

3.2 Předmět plnění dle této Smlouvy zahrnuje zejména tyto činnosti:

Služba poskytnutí infrastruktury PaaS pro provoz PÚEP

3.2.1 Předmětem služby infrastruktury PaaS je poskytování výpočetního výkonu na platformě MS Azure Stack (dále také „***AzS***“) v režimu 24x7, jehož součástí je:

3.2.1.1 Přiřazená kapacita výpočetního výkonu v prostředí virtualizované infrastruktury MS Azure Stack Poskytovatele pro požadovaný počet virtuálních serverů dle požadovaných parametrů dle **Přílohy č. 1** Smlouvy. Objednatel bude mít možnost komunikace z a do prostředí AzS Poskytovatele.

3.2.2 Předmětem služby infrastruktury PaaS je dále poskytnutí Služby správy operačního systému, které zahrnují:

3.2.2.1 Instalaci nezbytných operačních systémů – MS Windows Server a RHEL;

3.2.2.2 Instalaci verzí/patchů OS v pravidelných intervalech;

3.2.2.3 Změny konfigurací OS;

3.2.2.4 Instalaci kritických oprav OS;

3.2.2.5 Kontrolu existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;

3.2.2.6 Vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu);

3.2.2.7 Instalaci a konfiguraci nového software;

3.2.2.8 Instalaci a údržbu ovladačů a firmware hardware virtualizační platformy;

3.2.2.9 Správu účtů v OS;

3.2.2.10 Případné úpravy výkonnostních parametrů systému;

3.2.2.11 Správu souborového systému (filesystem, přístupová práva, kvóty a limity jeho použití);

3.2.2.12 Konzultace při poskytování podpory uživatelům Objednatele a jeho dodavatele aplikace PÚEP;

3.2.2.13 Údržbu dokumentace o konfiguraci OS;

3.2.2.14 Troubleshooting OS;

3.2.2.15 Hardening OS;

3.2.2.16 Testování změn provedených v OS;

3.2.2.17 Komunikaci a řešení problémů s externím supportem;

3.2.2.18 Konfigurace a nastavení firewallu a antiviru v prostředí OS.

3.2.3 Předmětem služby infrastruktury PaaS je dále poskytnutí Služby provozu databáze PostgreSQL na samostatném a dedikovaném databázovém serveru a jejíž součástí jsou následující provozní činnosti, které zahrnují:

3.2.3.1 Instalaci databázového serveru bez poskytnutí licence;

3.2.3.2 Administraci databáze (změny konfigurací databáze, správa účtů v databázi);

3.2.3.3 Instalaci patchů a kritických oprav;

3.2.3.4 Instalaci security patchů;

3.2.3.5 Upgrade a migraci databáze;

3.2.3.6 Definice zálohování a obnovy dat;

3.2.3.7 Vyhodnocování výstupů z monitoringu databáze (sledování výkonnostních parametrů a zatížení databáze);

3.2.3.8 Úpravy výkonnostních parametrů databáze;

3.2.3.9 Reportování výstupů z monitoringu na vyžádání;

3.2.3.10 Preventivní údržbu databázového serveru a databází;

3.2.3.11 Restarty databází dle požadavků Objednatele;

3.2.3.12 Odpovídání na technické dotazy Objednatele;

3.2.3.13 Údržbu dokumentace o konfiguraci databáze;

3.2.3.14 Troubleshooting databáze;

3.2.3.15 Testování změn provedených v databázi;

3.2.3.16 Komunikaci a řešení problémů s externím suportem.

3.2.4 Předmětem služby infrastruktury PaaS je dále poskytnutí Provozních služeb, které zahrnují:

3.2.4.1 Přípravu, konfiguraci a správu síťové infrastruktury, vč. provozního IT monitoringu a logování;

3.2.4.2 Poskytnutí konektivity do internetu z DC Poskytovatele s alokovanou kapacitou 50 Mbps vč. nastavení pravidel stavového firewallu a poskytnutí služeb loadbalancingu a SSL terminace;

3.2.4.3 Poskytnutí vzdáleného přístupu ke zdrojům výpočetního výkonu prostřednictvím privátní VPN pro celkem 5 uživatelů Objednatele;

3.2.4.4 Zajištění konektivity do CMS2 pro přenos dat z poskytovaných serverů do infrastruktury Objednatele;

3.2.4.5 Zajištění logování pomocí služby centrálního log managementu, které se provozuje v prostředí Poskytovatele infrastruktury pro sběr, uchování a analýzu logů, které se ze zdrojů logů sbírají pomocí standardních rozhraní. Prostředí je rozděleno do dvou základních vrstev, datová pro sběr, transformaci a ukládání logů, a následně prezentační pro analytickou práci a interpretaci logů nebo událostí dle předpřipravených postupů, filtrů a grafů. Základní přístup do systému lze pro Objednatele poskytnout pro analytické účely v read-only. Připojení jednotlivých zdrojů logů do nástroje log managementu, případně úpravy jejich prezentace nebo reportů potřebných pro provoz řešení, se zajišťuje v součinnosti mezi Objednatelem a Poskytovatelem;

3.2.4.6 Přípravu, konfiguraci a správu zálohování, realizované formou snapshotů image disků jednotlivých serverů;

3.2.4.7 Dohled nad kvalitou poskytované služby zahrnuje zejména – vyhodnocování dostupnosti služby a pravidelný měsíční reporting.

(3.2.1 a 3.2.4 dále jen „***Služba infrastruktury PaaS***").

3.2.5 Předmětem plnění je závazek Poskytovatele poskytovat na vlastní náklady a nebezpečí Objednateli řádně a včas Službu infrastruktury PaaS.

3.2.6 Detailní popis Služby infrastruktury PaaS, její kvalitativní parametry, rozdělení odpovědností a řízení incidentů je uveden v **Příloze č. 1** této Smlouvy.

3.2.7 Předmětem plnění je dále závazek Poskytovatele k přípravě Služby infrastruktury PaaS, která zahrnuje následující činnosti:

3.2.7.1 Příprava subskripce v prostředí AzS v DC Vápenka

- Vytvoření a konfigurace jednotlivých zdrojů výpočetního výkonu dle definovaných plánů;
- Vytvoření a konfigurace síťových prostupů z AzS do prostředí DC Poskytovatele.

3.2.7.2 Konfigurační práce na síťové vrstvě

- Konfigurace síťových prostupů a komunikací na FW;
- Konfigurace loadbalancerů;
- Konfigurace klientských VPN přístupů;
- Konfigurace konektivity do CMS2.

3.2.7.3 Příprava OS a databází

- Instalace operačních systémů MS Windows Server a RHEL na poskytované servery dle požadavku Objednatele;
- Vytvoření nezbytných účtů v rámci OS a zajištění přístupu pro Objednatele vč. jeho dodavatele;
- Instalace databázového prostředí PostgreSQL;
- Vytvoření nezbytných databázových účtů a zajištění přístupu pro Objednatele vč. jeho dodavatele.

(3.2.7 dále jen „***Příprava služby infrastruktury PaaS***").

Služba bezpečnostní monitoring – ověřovací provoz

3.2.8 Předmětem Služby bezpečnostní monitoring – ověřovací provoz je příprava nasazení Služby bezpečnostního monitoringu. Požadované parametry dostupnosti služby jsou garantovány až po ukončení ověřovacího provozu. Služba bude probíhat od termínu uvedeného ve vstupní analýze až do doby uzavření dodatku Smlouvy na službu dle odst. 5.1.2 Smlouvy.

Služba bezpečnostní monitoring

3.2.9 Předmětem služby bezpečnostní monitoring je nepřetržitý bezpečnostní monitoring v režimu 24x7 aktiv Objednatele definovaných v Příloze č. 2 této Smlouvy.

3.2.10 Typy záznamů, se kterými Služba bezpečnostní monitoring pracuje, jsou zejména:

3.2.10.1 logy operačních systémů;

3.2.10.2 logy aplikací.

3.2.11 Předmětem plnění je závazek Poskytovatele poskytovat na vlastní náklady a nebezpečí Objednateli řádně a včas Službu bezpečnostního monitoringu.

3.2.12 Detailní popis Služby bezpečnostní monitoring, její kvalitativní parametry, rozdělení odpovědností a řízení incidentů je uveden v **Příloze č. 2** této Smlouvy.

3.2.13 Předmětem plnění je dále závazek Poskytovatele k přípravě Služby bezpečnostního monitoringu, která zahrnuje následující činnosti:

3.2.13.1 Zpracování vstupní analýzy Poskytovatelem, která bude předaná Objednateli.

3.2.13.2 Nastavení služby bezpečnostního monitoringu na základě vstupní analýzy.

(3.2.13 dále jen „***Příprava služby bezpečnostního monitoringu***"). O Přípravě služby bezpečnostního monitoringu bude mezi Smluvními stranami podepsán akceptační protokol (dále jen „***Akceptační protokol***", jehož vzor tvoří Příloha č. 5 Smlouvy)

(Služba infrastruktury PaaS a Služba bezpečnostní monitoring dále společně také jako „***Služby***")

(článek 3.2.7 Příprava služby infrastruktury PaaS a článek 3.2.13 Příprava služby bezpečnostního monitoringu dále společně také jako „***Příprava služeb***").

3.3 Objednatel se zavazuje zaplatit Poskytovateli za řádně a včas realizované plnění sjednanou cenu dle Smlouvy.

IV. DOBA A MÍSTO PLNĚNÍ

4.1 Místem plnění dle této Smlouvy je sídlo Poskytovatele: Na Vápence 915/14, 130 00 Praha 3 a dále provozovna Poskytovatele na adrese Československé armády 1060/81, 250 91 Zeleneč. Pokud to povaha plnění Smlouvy umožňuje, je Poskytovatel oprávněn poskytovat plnění dle Smlouvy také vzdáleným přístupem, není-li nezbytné nebo vhodné výkon takového plnění zajistit on-site.

4.2 Služba infrastruktury PaaS, Služba bezpečnostního monitoringu – ověřovací provoz a Služba bezpečnostního monitoringu bude poskytována ode dne oznámení Poskytovatele o Zřízení Služby/Služeb, které bude odesláno prostřednictvím datové schránky Objednatele, ID datové schránky: h93aayw (dále jen „***Oznámení o Zřízení služby***") do konce platnosti Smlouvy. Poskytovatel se zavazuje zaslat Oznámení o Zřízení služby infrastruktury PaaS a služby bezpečnostního monitoringu – ověřovací provoz nejpozději do 31. 12. 2024 a současně se zavazuje zaslat Oznámení o Zřízení služby bezpečnostního monitoringu nejpozději do 31. 12. 2025.

V. CENA A PLATEBNÍ PODMÍNKY

5.1 Objednatel se zavazuje hradit měsíčně **cenu za Služby** ve výši 164 965 Kč bez DPH, tj. 199 607,65 Kč vč. DPH, která se skládá z:

5.1.1 **Ceny za Službu infrastruktury PaaS** a **Službu bezpečnostního monitoringu – infrastruktura** činí **135 548 Kč** bez DPH, tj. **164 013,08 Kč** včetně DPH ve výši 21 %;

5.1.2 **Cena za Službu bezpečnostního monitoringu – Aplikace** bude stanovena po dokončení Přípravy služby bezpečnostního monitoringu na základě vstupní analýzy a ověření provozu. Ke stanovení ceny za Službu bezpečnostního monitoringu se Smluvní strany zavazují uzavřít dodatek Smlouvy.

5.1.3 **Cena za Službu bezpečnostního monitoringu – ověřovací provoz – Aplikace** činí **29 417 Kč** bez DPH, tj. **35 594,57 Kč** včetně DPH ve výši 21 %. Cena se bude platit měsíčně od termínu uvedeného ve vstupní analýze až do doby uzavření dodatku Smlouvy na službu dle odst. 5.1.2

(vše dohromady dále jako „***Cena za Služby***")

5.2 Smluvní strany se dohodly, že v případě, kdy nebude Služba infrastruktury PaaS a Služba bezpečnostního monitoringu poskytovány po celý kalendářní měsíc (v případě zahájení nebo ukončení poskytování Služby), se Cena za Služby poměrně krátí, a to s přesností na celé dny trvání poskytování Služeb.

5.3 Cena za Službu infrastruktury PaaS a Službu bezpečnostního monitoringu bude hrazena poprvé za měsíc, ve kterém bylo skutečně započato s poskytováním dané Služby, tj. dnem zaslání Oznámení o Zřízení Služby/Služeb. Cena za Službu Bezpečnostní monitoring – ověřovací provoz bude hrazena od data uvedeného ve Vstupní analýze a v Akceptačním protokolu ke vstupní analýze.

5.4 Objednatel se dále zavazuje jednorázově uhradit **cenu za Přípravu služby** ve výši 752 919 Kč bez DPH, tj. 911 031,99 Kč vč. DPH se skládá z:

5.4.1 **Ceny za Přípravu služby infrastruktury PaaS** a **Služby bezpečnostního monitoringu – infrastruktura** činí **523 619 Kč** bez DPH, tj. **633 578,99 Kč** včetně DPH ve výši 21 %;

5.4.2 **Cena za Přípravu Služby bezpečnostní monitoring – Aplikace** činí **229 300 Kč** bez DPH, tj. **277 453 Kč** včetně DPH ve výši 21 %;

(vše dohromady dále jako „***Cena za přípravu Služby/Služeb***")

5.5 Cena za přípravu Služby infrastruktury PaaS bude vyfakturována jednorázově na základě Oznámení o zřízení Služby. Cena za přípravu Služby bezpečnostního monitoringu bude vyfakturována jednorázově na základě Akceptačního protokolu.

5.6 Ceny uvedené v tomto článku Smlouvy, jsou uvedeny jako maximální, nejvýše přípustné, nepřekročitelné a zahrnující veškeré náklady Poskytovatele nutné k řádnému a včasnému splnění předmětu Smlouvy (např. správní a místní poplatky, vedlejší náklady apod.). Cenu plnění je možné upravit pouze za níže specifikovaných podmínek.

5.7 Strany se dohodly, že pokud dojde v průběhu plnění Smlouvy ke změně zákonné sazby DPH stanovené pro plnění předmětu Smlouvy, bude tato sazba promítnuta do všech cen uvedených ve Smlouvě s DPH a Poskytovatel je od okamžiku nabytí účinnosti změny zákonné sazby DPH povinen účtovat platnou sazbu DPH. O této skutečnosti není nutné uzavírat dodatek ke Smlouvě.

5.8 Poskytovatel odpovídá za to, že sazba DPH je stanovena v souladu s platnými právními předpisy.

5.9 Cena dle odst. 5.4 této Smlouvy je splatná jednorázově v měsíci, kdy Poskytovatel zahájil poskytován Služeb. Cena dle odst. 5.4 může být vyfakturována společně s prvním vyúčtováním služeb dle odst. 5.1 dle této Smlouvy.

5.10 Cena dle odst. 5.1 této Smlouvy je splatná měsíčně zpětně. Poskytovatel je oprávněn vystavit daňový doklad (fakturu) na základě akceptovaného Záznamu o poskytnutí služeb.

5.11 Za den uskutečnění zdanitelného plnění dle článku 5.9 a 5.10 se považuje poslední den kalendářního měsíce, ve kterém byla služba poskytnuta.

5.12 Daňový doklad (dále jen „***Faktura***“) Poskytovatel odešle do pěti (5) kalendářních dnů od jeho vystavení Objednateli spolu s požadovanými přílohami elektronicky do datové schránky Objednatele: ID datové schránky: h93aayw.

5.13 Splatnost řádně vystavené Faktury, obsahující stanovené náležitosti, musí činit nejméně 30 (slovy: třicet) kalendářních dnů ode dne jejich doručení Objednateli.

5.14 Faktura musí obsahovat evidenční číslo Smlouvy a veškeré údaje vyžadované právními předpisy, zejména ustanovením § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „***zákon o DPH***“), zákona č. 563/1991, o účetnictví ve znění pozdějších předpisů a § 435 OZ. Poskytovatel je povinen k Faktuře k Ceně Služby připojit akceptovaný Záznam o poskytnutí Služeb, jehož vzor tvoří **Přílohu č. 4** Smlouvy.

5.15 Nebude-li Faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo přílohu nebo bude-li chybně vyúčtována cena nebo DPH, je Objednatel oprávněn Fakturu před uplynutím lhůty splatnosti bez zaplacení vrátit Poskytovateli k provedení opravy s vyznačením důvodu vrácení. Poskytovatel provede opravu vystavením nové Faktury. Odesláním vadné Faktury Poskytovateli přestává běžet původní lhůta splatnosti, přičemž nová lhůta splatnosti bude stanovena v souladu s odst. 5.12 Smlouvy.

5.16 Všechny částky poukazované v Kč vzájemně Stranami na základě Smlouvy musí být prosté jakýchkoliv bankovních poplatků nebo jiných nákladů spojených s převodem na jejich účty.

5.17 Objednatel neposkytuje Poskytovateli na plnění předmětu Smlouvy jakékoliv zálohy.

5.18 Faktura se považuje za uhrazenou dnem odepsání příslušné finanční částky z účtu Objednatele ve prospěch účtu Poskytovatele.

5.19 Smluvní strany se dohodly, že pokud bude v okamžiku uskutečnění zdanitelného plnění správcem daně zveřejněna způsobem umožňujícím dálkový přístup skutečnost, že poskytovatel zdanitelného plnění (Poskytovatel) je nespolehlivým plátcem ve smyslu § 106a Zákona o DPH, nebo má-li být platba za zdanitelné plnění uskutečněné Poskytovatelem v tuzemsku zcela nebo z části poukázána na bankovní účet vedený poskytovatelem platebních služeb mimo tuzemsko, je příjemce zdanitelného plnění (Objednatel) oprávněn část ceny odpovídající dani z přidané hodnoty zaplatit přímo na bankovní účet správce daně ve smyslu § 109a Zákona o DPH. Na bankovní účet Poskytovatele bude v tomto případě uhrazena část ceny odpovídající výši základu daně z přidané hodnoty. Úhrada ceny plnění (základu daně) provedená Objednatelem v souladu s ustanovením tohoto odstavce Smlouvy bude považována za řádnou úhradu ceny plnění poskytnutého dle této Smlouvy. Zároveň je Objednatel povinen Poskytovatele o takové úhradě bezprostředně po jejím uskutečnění písemně informovat.

5.20 Bankovní účet uvedený na daňovém dokladu, na který bude ze strany Poskytovatele požadována úhrada ceny za poskytnuté zdanitelné plnění, musí být Poskytovatelem zveřejněn způsobem umožňujícím dálkový přístup ve smyslu § 96 Zákona o DPH. Smluvní strany se výslovně dohodly, že pokud číslo bankovního účtu Poskytovatele, na který bude ze strany Poskytovatele požadována úhrada ceny za poskytnuté zdanitelné plnění dle příslušného daňového dokladu, nebude zveřejněno způsobem umožňujícím dálkový přístup ve smyslu § 96 Zákona o DPH a cena za poskytnuté zdanitelné plnění dle příslušného daňového dokladu přesahuje limit uvedený v § 109 odst. 2 písm. C) Zákona o DPH, je Objednatel oprávněn zaslat daňový doklad zpět Poskytovateli k opravě. V takovém případě se doba splatnosti zastavuje a nová doba splatnosti počíná běžet dnem doručení opraveného daňového dokladu Objednateli s uvedením správného bankovního účtu Poskytovatele, tj. bankovního účtu zveřejněného správcem daně.

5.21 Poskytovatel je povinen bezprostředně, nejpozději do dvou pracovních dnů od zjištění insolvence nebo hrozby jejího vzniku, oznámit takovou skutečnost prokazatelně Objednateli – příjemci zdanitelného plnění s uvedením data, kdy taková skutečnost nastala. Porušení této povinnosti je smluvními stranami považováno za podstatné porušení této Smlouvy.

5.22 Poskytovatel je oprávněn zvýšit každou z Cena za Služby dle této Smlouvy s účinností od 1. dubna 2026 a každého následujícího kalendářního roku o přírůstek průměrného ročního indexu spotřebitelských cen (dále jen „***Míra inflace***") vyhlášeného Českým statistickým úřadem za předcházející kalendářní rok. Pro vyloučení pochybností Smluvní strany sjednávají, že za účelem zvýšení Cen za Službu dle Míry inflace není nutné uzavírat dodatek ke Smlouvě, pouze zaslat oznámení o navýšení ceny vždy k 31. 3. daného kalendářního roku. V případě, že dojde k nesprávnému vyčíslení navýšení Ceny za Služby o přírůstek průměrného ročního indexu spotřebitelských cen, je Poskytovatel povinen Objednateli doúčtovat Cenu za Služby dle správného vyčíslení navýšení Ceny za Služby o přírůstek průměrného ročního indexu spotřebitelských cen, na základě opravného daňového dokladu.

VI. PŘEDÁNÍ, PŘEVZETÍ A AKCEPTCE

6.1 Hodnocení, kontrola plnění a akceptace úrovně poskytovaných Služeb, podle smluvně dohodnutých podmínek bude probíhat vždy za každý uplynulý kalendářní měsíc následujícím způsobem:

6.1.1 Kontrolu plnění bude provádět Objednatel na základě Zprávy o úrovni a rozsahu poskytovaných služeb za uplynulý kalendářní měsíc. Kritéria pro hodnocení úrovně poskytovaných Služeb jsou definována v **Příloze č. 1 a Příloze č. 2** této Smlouvy.

6.1.2 Poskytovatel předloží Objednateli písemný Záznam o poskytnutí Služeb za uplynulý kalendářní měsíc, vždy do pátého (5.) pracovního dne následujícího kalendářního měsíce. Vzor Záznamu tvoří Příloha č. 3 Smlouvy.

6.1.3 Poskytovatel předloží Objednateli písemnou Zprávu o úrovni a rozsahu poskytovaných služeb za uplynulý kalendářní měsíc, vždy do desátého (10.) pracovního dne následujícího kalendářního měsíce.

6.1.4 Objednatel ve lhůtě pěti (5) pracovních dnů od předložení Zprávy o úrovni a rozsahu poskytovaných služeb zpracuje k této Zprávě o úrovni a rozsahu poskytovaných služeb písemné stanovisko.

6.1.5 Objednatel je povinen ve lhůtě pěti (5) pracovních dnů od předložení Záznamu o poskytnutí služeb tento záznam podepsat. V případě, že nebude Záznam o poskytnutí služeb ve výše uvedené lhůtě pěti pracovních dnů podepsán, považuje se Objednatelem akceptovaný.

6.1.6 V případě, že Objednatel bude mít výhrady k obsahu Zprávy o úrovni a rozsahu poskytovaných služeb, je Poskytovatel povinen zjednat nápravu cestou odstranění výhrad uvedených ve Zprávě o úrovni a rozsahu poskytovaných služeb ve lhůtě čtrnácti (14) kalendářních dní od oznámení, pokud se smluvní strany nedohodnou jinak. Po uplynutí této lhůty zahajuje Poskytovatel novou akceptační proceduru opětovným předáním Zprávy o úrovni a rozsahu poskytovaných služeb.

6.2 Lhůty uvedené v tomto článku Smlouvy mohou být dodatečně upraveny pouze po vzájemné písemné dohodě obou smluvních stran bez nutnosti uzavřít dodatek k této Smlouvě.

VII. DALŠÍ PRÁVA A POVINNOSTI STRAN

7.1 Poskytovatel se dále zavazuje:

7.1.1 poskytovat řádně a včas plnění dle Smlouvy bez faktických a právních vad;

7.1.2 postupovat při realizaci plnění s odbornou péčí, podle nejlepších znalostí a schopností, sledovat a chránit oprávněné zájmy Objednatele a postupovat v souladu s jeho pokyny a interními předpisy souvisejícími s plněním dle této Smlouvy (či jeho dílčí částí), které Objednatel Poskytovateli poskytne, nebo s pokyny jím pověřených osob;

7.1.3 bez zbytečného odkladu oznámit Objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky plnění. Zejména je povinen neprodleně písemně oznámit Objednateli změny svého majetkoprávního postavení, jako je např. přeměna společnosti, snížení základního kapitálu, vstup do likvidace, úpadek či prohlášení konkurzu;

7.1.4 informovat bezodkladně Objednatele o jakýchkoliv zjištěných překážkách plnění dle Smlouvy, byť by za ně Poskytovatel neodpovídal, o vznesených požadavcích orgánů státního dozoru a o uplatněných nárocích třetích osob, které by mohly plnění dle Smlouvy ovlivnit;

7.1.5 poskytnout Objednateli veškerou nezbytnou součinnost k naplnění účelu Smlouvy;

7.1.6 na žádost Objednatele spolupracovat či poskytnout maximální součinnost dalším dodavatelům Objednatele;

7.1.7 informovat Objednatele na jeho žádost o průběhu realizace plnění a akceptovat jeho doplňující pokyny a připomínky k realizaci plnění;

7.1.8 použít veškeré podklady předané mu Objednatelem pouze pro účely Smlouvy a zabezpečit jejich řádné vrácení Objednateli, bude-li to objektivně možné vzhledem k jejich povaze a způsobu použití; a

7.1.9 poskytnout Objednateli veškeré údaje a informace potřebné ke splnění povinností Objednatele týkajících se uveřejňování údajů a informací o VZ dle platných právních předpisů.

7.2 Objednatel se dále zavazuje:

7.2.1 poskytovat Poskytovateli na základě jeho konkrétního písemného vyžádání úplné, pravdivé a včasné informace potřebné k řádnému a včasnému plnění Poskytovatele dle Smlouvy;

7.2.2 na základě konkrétního písemného vyžádání Poskytovatele zabezpečit účast pracovníků Objednatele či jím určených osob na pracovních schůzkách či na základě takové žádosti Poskytovatele zabezpečit potřebné technicko-organizační podmínky vyplývající ze Smlouvy;

7.2.3 poskytnout Poskytovateli součinnost potřebnou k řádné a včasné realizaci předmětu Smlouvy;

VIII. PODDODAVATELÉ, OPRÁVNĚNÉ OSOBY

8.1 Poddodavatelé

8.1.1 Poskytovatel se zavazuje plnění předmětu Smlouvy provést sám, nebo s využitím poddodavatelů.

8.1.2 Zadání provedení části plnění dle Smlouvy poddodavateli Poskytovatelem nezbavuje Poskytovatele jeho výlučné odpovědnosti za řádné provedení plnění dle Smlouvy vůči Objednateli. Poskytovatel odpovídá Objednateli za plnění předmětu Smlouvy, které svěřil poddodavateli, ve stejném rozsahu, jako by jej poskytoval sám.

8.2 Oprávněné osoby

8.2.1 Každá ze Stran dále jmenuje oprávněné osoby, které budou vystupovat jako zástupci Stran. Oprávněné osoby zastupují Stranu ve smluvních, projektových a technických záležitostech souvisejících s plněním předmětu Smlouvy.

8.2.2 Oprávněné osoby budou oprávněny činit rozhodnutí závazná pro Strany ve vztahu k Smlouvě v rámci své pravomoci. Oprávněné osoby, nejsou-li statutárními orgány, však nejsou oprávněny provádět změny ani zrušení Smlouvy s výjimkou oprávnění výslovně ve Smlouvě definovaných, nebude-li jim udělena speciální plná moc. Oprávněné osoby ve věcech technických jsou mj. oprávněny k předávání, přebírání a akceptování Služeb za příslušnou smluvní stranu.

8.2.3 Oprávněnými osobami za Objednatele jsou:

8.2.3.1 [redacted]

8.2.3.2 ve věcech technických:

[redacted]

8.2.4 Oprávněnými osobami za Poskytovatele jsou:

8.2.4.1 [redacted]

8.2.4.2

8.2.4.3

8.2.5 Každá ze Stran má právo změnit jí jmenované oprávněné osoby, musí však o každé změně vyrozumět písemně druhou Stranu. Změna oprávněných osob je vůči druhé Straně účinná okamžikem, kdy o ní byla písemně vyrozuměna. Pro případ jakékoliv změny těchto osob se Smluvní strany dohodly, že není potřeba uzavírat tomu odpovídající dodatek Smlouvy.

IX.ODPOVĚDNOST ZA ŠKODU

9.1 Strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Strany nesou odpovědnost za škodu dle platných právních předpisů a Smlouvy.

9.2 Poskytovatel se zároveň zavazuje Objednatele odškodnit za jakékoliv škody, které Objednateli v důsledku porušení povinností Poskytovatele vzniknou na základě pravomocného rozhodnutí soudu či jiného státního orgánu.

9.3 Žádná ze Stran není povinna nahradit škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Strany. V případě, že Objednatel poskytl Poskytovateli chybné zadání a Poskytovatel s ohledem na svou povinnost provést plnění dle Smlouvy či jeho část s odbornou péčí mohl a měl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.

9.4 Žádná ze Stran není odpovědná za škodu vzniklou porušením povinnosti ze Smlouvy, prokáže-li, že mu ve splnění povinnosti ze Smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá ze škůdcových osobních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním povinnosti ze Smlouvy v prodlení, ani překážka, kterou byl škůdce podle Smlouvy povinen překonat, ho však povinnosti k náhradě nezprostí. Strany se zavazují upozornit druhou stranu bez zbytečného odkladu na vzniklé překážky bránící řádnému plnění Smlouvy a dále se zavazují k vyvinutí maximálnímu úsilí k jejich odvrácení a překonání.

9.5 Výše náhrady škody či jiné újmy se řídí OZ a její maximální výše je omezena částkou 5 000 000,00 Kč (slovy: pět milionů korun českých).

9.6 Žádná ze smluvních stran neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany. Žádná ze smluvních stran neodpovídá za škodu vzniklou neplněním závazku zapříčiněným výlučně v důsledku prodlení druhé smluvní strany.

9.7 Poskytovatel se zavazuje, že bude mít po celou dobu účinnosti Smlouvy sjednánu pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Poskytovatelem třetí osobě s limitem pojistného plnění minimálně ve výši 10 000 000,00 Kč (slovy: deset milionů korun českých). Poskytovatel je povinen předat kopii pojistného certifikátu (pojistné smlouvy) Objednateli před podpisem Smlouvy a dále kdykoliv na vyžádání Objednatele, a to bez zbytečného odkladu, nejpozději však do 5 (slovy: pěti) pracovních dnů od doručení písemné žádosti Objednatele.

X. SANKČNÍ UJEDNÁNÍ

10.1 Strany se dohodly, že:

10.1.1 v případě porušení v povinnosti Poskytovatele udržovat v platnosti a účinnosti po celou dobu účinnosti Smlouvy pojistnou smlouvu dle odst. 9.7 Smlouvy vzniká Objednateli nárok na smluvní pokutu ve výši 100 000,00 Kč (slovy: jedno sto tisíc korun českých) za každý i započatý měsíc, v němž nebude mít uzavřenou pojistnou smlouvu se stanovenými parametry;

10.1.2 v případě, že Poskytovatel nesplní základní parametr roční dostupnosti Služby infrastruktury PaaS uvedený v článku 4 **Přílohy č. 1** Smlouvy, je Objednatel oprávněn požadovat smluvní pokutu ve výši 500,00 Kč (slovy: pět set korun českých) za každou započatou hodinu nad stanovený parametr roční dostupnosti Služby infrastruktury PaaS;

10.1.3 v případě, že Poskytovatel nesplní základní parametr roční dostupnosti Služby bezpečnostního monitoringu uvedený v článku 3 **Přílohy č. 2** Smlouvy, je Objednatel oprávněn požadovat smluvní pokutu ve výši 100,00 Kč (slovy: sto korun českých) za každou započatou hodinu nad stanovený parametr roční dostupnosti Služby bezpečnostního monitoringu;

10.1.4 V případě porušení kterékoli povinnosti podle čl. XI této Smlouvy je smluvní strana, která povinnost porušila, povinna zaplatit druhé smluvní straně smluvní pokutu ve výši 100 000,00 Kč (slovy: jedno sto tisíc korun českých) za každé jednotlivé prokázané porušení povinnosti.

10.2 Zaplacením smluvní pokuty není jakkoliv dotčen nárok Objednatele na náhradu škody; nárok na náhradu škody je Objednatel oprávněn uplatnit vedle smluvní pokuty v plné výši. Zaplacením smluvní pokuty či poskytnutím slevy z ceny není dotčeno splnění povinnosti, která je prostřednictvím smluvní pokuty zajištěna.

10.3 Celková výše smluvních pokut za dobu trvání Smlouvy je omezena částkou 2 000 000,00 Kč (slovy: dva miliony korun českých).

10.4 V případě prodlení kterékoliv Strany se zaplacením peněžité částky vzniká oprávněné straně nárok na úrok z prodlení v zákonné výši počítaný z dlužné částky za každý i započatý den prodlení. Tím není dotčen ani omezen nárok na náhradu vzniklé škody.

10.5 Vyúčtování smluvní pokuty / úroků z prodlení podle příslušných ustanovení této Smlouvy – penalizační faktura, musí být druhé Straně zasláno způsobem prokazujícím doručení, nejlépe datovou zprávou dle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Smluvní pokuta / úroky z prodlení jsou splatné ve lhůtě třiceti (30) kalendářních dnů ode dne doručení penalizační faktury. Úhrada smluvní pokuty / úroků z prodlení se provádí bankovním převodem na účet oprávněné Strany uvedený v penalizační faktuře. Částka se považuje za zaplacenou okamžikem jejího připsání ve prospěch účtu oprávněné Strany.

XI. OCHRANA NEVEŘEJNÝCH INFORMACÍ

11.1 Strany jsou si vědomy toho, že v rámci plnění závazků ze Smlouvy:

11.1.1 mohou si vzájemně vědomě nebo opominutím poskytnout informace, které budou považovány za neveřejné (dále jen „***Neveřejné informace***“);

11.1.2 mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé Strany nebo i jejím opominutím přístup k Neveřejným informacím druhé Strany.

11.2 Strany se dohodly, že Neveřejné informace nikomu neprozradí a přijmou taková opatření, která znemožní jejich přístupnost třetím osobám. Ustanovení předchozí věty se nevztahuje na případy, kdy:

11.2.1 Strany mají povinnost stanovenou právním předpisem, a/nebo

11.2.2 takové informace sdělí osobám, které mají ze zákona stanovenou povinnost mlčenlivosti vztahující se k těmto informacím, a/nebo

11.2.3 se takové informace stanou veřejně známými či dostupnými jinak než porušením povinností vyplývajících z tohoto článku Smlouvy.

11.3 Za třetí osoby dle odst. 11.2 Smlouvy se nepovažují:

11.3.1 zaměstnanci Stran a osoby v obdobném postavení;

11.3.2 orgány Stran a jejich členové;

11.3.3 poradci Stran;

11.3.4 ve vztahu k Neveřejným informacím Objednatele poddodavatelé Poskytovatele; a ve vztahu k Neveřejným informacím Poskytovatele externí dodavatelé Objednatele, a to i potenciální;

za předpokladu, že se podílejí na plnění Smlouvy nebo na plnění spojeném s plněním dle Smlouvy, Neveřejné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění Neveřejných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny Stranám ve Smlouvě.

11.4 Veškeré informace poskytnuté Objednatelem Poskytovateli se považují za Neveřejné informace, není-li stanoveno jinak. Veškeré informace poskytnuté Poskytovatelem Objednateli se považují za Neveřejné informace, pouze pokud na jejich důvěrnost Poskytovatel Objednatele předem upozornil v souladu s článkem 1.9 Smlouvy.

11.5 V případě uplatnění smluvních pokut a náhrady škody není dotčena hmotná a trestní odpovědnost fyzických osob, které za Poskytovatele jednaly a závazek mlčenlivosti a ochrany Neveřejných informací nedodržely.

11.6 Závazek k mlčenlivosti a ochraně Neveřejných informací je platný bez ohledu na ukončení účinnosti Smlouvy.

XII.ZMĚNOVÉ ŘÍZENÍ

12.1 Kterákoliv ze Smluvních stran je oprávněna písemně navrhnout změny Služeb a parametrů jejich poskytování, a to prostřednictvím požadavku zaslaného prostřednictvím e-mailu Oprávněné osobě příslušné Smluvní strany (dále jen „***Změnový požadavek***"). Žádná ze Smluvních stran není povinna navrhované změny akceptovat.

12.2 Poskytovatel se zavazuje provést hodnocení dopadů navrhovaných změn Služeb z hlediska vhodnosti, termínů plnění, součinnosti Smluvních stran a ceny. Poskytovatel se zavazuje provést hodnocení bez zbytečného odkladu, nejpozději do 10 pracovních dnů ode dne doručení Změnového požadavku Objednateli, není-li Smluvními stranami dohodnuto jinak.

12.3 Smluvní strany se zavazují za účelem potvrzení změn dle tohoto článku uzavřít dodatek ke Smlouvě, kterým budou provedené změny do Smlouvy promítnuty, není-li ve Smlouvě výslovně sjednáno jinak. V závislosti na takovém dodatku může být upraven požadovaný rozsah plnění Služeb, termíny plnění Služeb, cena Služeb, platební podmínky, součinnost Objednatele atd.

12.4 Obě Smluvní strany se zavazují případné změny či doplňky této Smlouvy činit písemně.

XIII.MOŽNOSTI UKONČENÍ SMLOUVY

13.1 Smlouva může být ukončena písemnou dohodou Smluvních stran.

13.2 Každá ze smluvních stran je oprávněna vypovědět smlouvu bez udání důvodu s výpovědní dobou 12 měsíců. Výpovědní doba plyne od prvního dne následujícího po měsíci, ve které byla výpověď Smlouvy doručena druhé Smluvní straně.

13.3 Objednatel je oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Poskytovatelem v případech, ve kterých tak stanoví Smlouva.

13.4 Objednatel je rovněž oprávněn odstoupit od Smlouvy v případě, že:

13.4.1 v insolvenčním řízení bude zjištěn úpadek Poskytovatele nebo insolvenční návrh bude zamítnut pro nedostatek majetku Poskytovatele v souladu se zněním zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů. Objednatel je rovněž oprávněn odstoupit od Smlouvy v případě, že Poskytovatel vstoupí do likvidace; nebo

13.4.2 proti Poskytovateli je zahájeno trestní stíhání pro trestný čin podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů;

13.4.3 dojde k významné změně kontroly nad Poskytovatelem, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle ust. § 71 a násl. Zákona o obchodních korporacích, či ekvivalentní postavení;

13.4.4 Poskytovatel nebude nejpozději k 1. lednu 2025 zapsán v katalogu cloud computingu vedeného Digitální informační agenturou jako poskytovatel cloudových služeb bezpečnostní úrovně č. 4, a to v souladu s vyhláškou č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu.

13.5 Poskytovatel je oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Objednatelem, přičemž za podstatné porušení Smlouvy se bude považovat prodlení Objednatele s úhradou ceny za plnění předmětu Smlouvy delší než 30 (slovy: třicet) kalendářních dnů, pokud Objednatel nezjedná nápravu ani do 10 (slovy: deseti) pracovních dnů od doručení písemného oznámení Poskytovatele o takovém prodlení se žádostí o jeho nápravu.

13.6 Odstoupení od Smlouvy ze strany Objednatele nesmí být spojeno s uložením jakékoliv sankce k tíži Objednatele.

13.7 Strany se dále dohodly, že odstoupení od Smlouvy musí být písemné, jinak je neplatné. Odstoupení je účinné ode dne, kdy bylo doručeno druhé Straně. Strany se dohodly, že v případě odstoupení od Smlouvy se nevrací Poskytovatelem již provedené a Objednatelem akceptované plnění dle Smlouvy.

13.8 Ukončením Smlouvy nejsou dotčena ustanovení o odpovědnosti za škodu, nároky na uplatnění smluvních pokut, o ochraně Neveřejných informací a ostatních práv a povinností založených Smlouvou, která mají podle zákona nebo Smlouvy trvat i po jejím zrušení.

13.9 V případě ukončení Smlouvy se Poskytovatel zavazuje vypracovat a předložit Plán ukončení provozu vč. předání dat Objednateli.

XIV. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

14.1 Strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Strany jsou povinny informovat druhou Stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění Smlouvy, např. změně sídla, právní formy, změně bankovního spojení, zrušení registrace k DPH apod.

14.2 Strany jsou povinny plnit své závazky vyplývající ze Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků.

14.3 Veškerá komunikace mezi Stranami bude probíhat postupem stanoveným v článku VIII Smlouvy.

14.4 Oznámení mezi Stranami, která se vztahují k Smlouvě nebo která mají být učiněna na základě Smlouvy, musí být učiněna v písemné (papírové nebo elektronické) podobě a druhé Straně doručena osobně, doporučeným dopisem či jinou formou registrovaného poštovního styku na adresu uvedenou na titulní stránce Smlouvy, nebo datovou schránkou. Běžná pracovní komunikace může být vedena prostřednictvím elektronické pošty.

14.5 Písemnosti doručované v souvislosti se Smlouvou (oznámení) se považují za doručené 2. pracovní den po jejich prokazatelném odeslání.

14.6 Ukládá-li Smlouva předat některý dokument, musí být předán také v elektronické podobě.

14.7 Strany se zavazují, že v případě změny svých kontaktních údajů (adresy, telefonní čísla a adresy elektronické pošty) budou o této změně písemně druhou Stranu informovat nejpozději do 3 (slovy: tří) pracovních dnů. Tato změna nevyžaduje uzavření dodatku Smlouvy.

XV. ZÁVĚREČNÁ USTANOVENÍ

15.1 Smlouva nabývá platnosti dnem jejího podpisu oběma Stranami a účinnosti dnem jejího uveřejnění v registru smluv dle ZoRS. Smlouva se uzavírá na dobu neurčitou.

15.2 Strany si podpisem Smlouvy sjednávají (pokud Smlouva nestanoví jinak), že závazky Smlouvou založené budou vykládány výhradně podle obsahu Smlouvy, bez přihlédnutí k jakékoli skutečnosti, která nastala a/nebo byla sdělena, jednou stranou druhé straně před uzavřením Smlouvy.

15.3 Smlouva představuje úplnou dohodu Stran o předmětu Smlouvy a všech náležitostech, které Strany měly a chtěly ve Smlouvě ujednat, a které považují za důležité pro závaznost Smlouvy. Žádný projev stran učiněný po uzavření Smlouvy nesmí být vykládán v rozporu s výslovnými ustanoveními Smlouvy a nezakládá žádný závazek žádné ze Stran. Smlouvu je možné měnit pouze písemnou dohodou Stran ve formě číslovaných dodatků Smlouvy, podepsaných oprávněnými zástupci obou Stran.

15.4 Strany si sdělily všechny skutkové a právní okolnosti, o nichž k datu podpisu Smlouvy věděly nebo vědět musely, a které jsou relevantní ve vztahu k uzavření Smlouvy. Kromě ujištění, které si Smluvní strany poskytly ve Smlouvě, nebude mít žádná ze Stran žádná další práva a povinnosti v souvislosti s jakýmikoliv skutečnostmi, které vyjdou najevo a o kterých neposkytla druhá Strana informace při jednání o Smlouvě. Výjimkou budou případy, kdy daná Strana úmyslně uvedla druhou Stranu ve skutkový omyl ohledně předmětu Smlouvy a případy taxativně stanovené Smlouvou.

15.5 Jednacím jazykem mezi Objednatelem a Poskytovatelem bude pro veškerá plnění vyplývající ze Smlouvy výhradně jazyk český, a to včetně veškeré dokumentace vztahující se k předmětu Smlouvy, není-li stanoveno jinak (u dokumentace Objednatel připouští rovněž anglický jazyk, a to u odborných výrazů a terminologie).

15.6 Je-li nebo stane-li se jakékoli ustanovení Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení Smlouvy. Strany se tímto zavazují nahradit do 5 (pěti) pracovních dnů po doručení výzvy druhé Strany jakékoli takové neplatné, nezákonné nebo nevynutitelné ustanovení ustanovením, které je platné, zákonné a vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.

15.7 Vztahy Stran Smlouvou výslovně neupravené se řídí českým právním řádem, zejména pak OZ a příslušnými právními předpisy souvisejícími. Veškeré případné spory ze Smlouvy budou v prvé řadě řešeny smírem. Pokud smíru nebude dosaženo během 30 (třiceti) dnů, všechny spory ze Smlouvy a v souvislosti s ní budou řešeny věcně a místně příslušným soudem v České republice.

15.8 Poskytovatel souhlasí s uveřejněním Smlouvy na profilu Objednatele a v registru smluv dle ZoRS.

15.9 Smlouva je vyhotovena v elektronické podobě v 1 (slovy: jednom) vyhotovení v českém jazyce s elektronickými podpisy obou Stran v souladu se zákonem č. 297/2016 Sb. O službách vytvářejících důvěru pro elektronické transakce ve znění pozdějších předpisů.

15.10 Nedílnou součástí Smlouvy jsou následující přílohy:

Příloha č. 1 – Specifikace Služby infrastruktury PaaS _KL001
Příloha č. 2 – Specifikace Služby bezpečnostního monitoringu_KL002
Příloha č. 3 – Záznam o poskytnutí Služeb
Příloha č. 4 – Zpráva o úrovni a rozsahu poskytovaných Služeb
Příloha č. 5 – Akceptační protokol

Smluvní strany shodně prohlašují, že si Smlouvu před jejím podpisem přečetly a že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, a že se dohodly o celém jejím obsahu, což stvrzují svými podpisy.

Za Poskytovatele: V Praze dne dle elektronického podpisu	Za Objednatele: V Praze dne dle elektronického podpisu
Mgr. Jakub Richter 1. zástupce generálního ředitele Státní pokladna Centrum sdílených služeb, s. p.	Mgr. Jan Čuřín Ředitel Národní bezpečnostní úřad

TECHNICKÁ SPECIFIKACE SLUŽBY

Katalogový list KL001

Název Služby	**Poskytnutí infrastruktury pro Portál úplného elektronického podání**

Obsahem tohoto katalogového listu je Služba poskytnutí infrastruktury (dále v tomto katalogovém listu jen „***Služba***") v datovém centru SPCSS (dále jako „Poskytovatel") pro provoz aplikace Portál úplného elektronického podání (dále jako „PÚEP") pro Národní bezpečnostní úřad (dále jako „Objednatel").

Služba bude provozována na úrovni PaaS, kdy Poskytopvatel zajistí provoz HW infrastruktury, operačních systémů a databází. Nabízená Služba bude splňovat 4. (tj. kritickou) bezpečnostní úroveň cloud computingu z důvodu ochrany osobních údajů žadatelů o bezpečnostní prověrky.

I.OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba poskytnutí infrastruktury (PaaS) je poskytována od data Oznámení o Zřízení služby po dobu neurčitou.

II.REŽIM POSKYTOVÁNÍ SLUŽBY

Jednotlivá prostředí budou poskytována v následujícím rozsahu doby poskytování služby:

Prostředí	Doba poskytování
Produkční	7x24
Testovací	7x24

III.POPIS ROZSAHU SLUŽBY

Předmětem Služby, dle tohoto Katalogového listu, je poskytování výpočetního výkonu, správa operačních systémů, správa databáze a související provozní služby na sdílené infrastruktuře Poskytovatele.

3.1 Poskytování Služby výpočetního výkonu

Poskytování výpočetního výkonu na platformě MS Azure Stack (dále také „AzS") bude realizováno prostřednictvím alokace zdrojů a kapacity v rámci AzS provozovaného Poskytovatelem pro požadovaný počet serverů. Objednatel díky Službě bude mít možnost komunikace z a do prostředí AzS Poskytovatele.

Platforma AzS funguje jako prostředí hyperkonvergované infrastruktury provozované v datových centrech Poskytovatele. Jako hlavní škálovatelná jednotka výpočetního výkonu je v prostředí AzS nabízen virtuální server v podobě plánu, kde každý takový plán má předem stanovenou výši parametrů virtualizovaného výpočetního výkonu (vCPU) a virtualizované RAM.

Pro účely provozu a využití platformy AzS budou pro Objednatele vytvořeny a zpřístupněny administrátory Poskytovatele následující zdroje dle požadavku Objednatele.

Službě přiřazené HW virtualizované prostředky	Plán v AzureStacku	Počet kusů
Produkční prostředí		
Aplikační server pro produkční prostředí s OS WIN 4 vCPU, 8 GB vRAM, 64 GB vHDD, 32 GB vHDD	AZS_B1_4_8	2
Databázový server pro produkční prostředí s OS RHEL 8 vCPU, 16 GB vRAM, 64 GB vHDD, 128 GB vHDD, 512 GB vHDD	AZS_C1_8_16	1
Formulářový server pro produkční prostředí s OS WIN 4 vCPU, 8 GB vRAM, 64 GB vHDD, 32 GB vHDD	AZS_B1_4_8	2
Testovací prostředí		
Aplikační server pro testovací prostředí s OS WIN 4 vCPU, 8 GB vRAM, 64 GB vHDD, 32 GB vHDD	AZS_B1_4_8	1
Databázový server pro testovací prostředí s OS RHEL 8 vCPU, 16 GB vRAM, 64 GB vHDD, 128 GB vHDD, 512 GB vHDD	AZS_C1_8_16	1
Formulářový server pro testovací prostředí s OS WIN 4 vCPU, 8 GB vRAM, 64 GB vHDD, 32 GB vHDD	AZS_B1_4_8	1

Součástí Služby jsou dále následující oblasti:

- Příprava, zprovoznění a správa infrastrukturních zdrojů, vč. provozního IT monitoringu a logování;
- Licence, instalace a správa operačních systémů – viz odst.3.2;
- Instalace a správa middleware – viz odst. 3.3.

3.2 Poskytování Služby správy operačního systému

Součástí této oblasti Služby jsou následující provozní činnosti:

- Instalace nezbytných operačních systémů – MS Windows Server a RHEL;
- Instalace verzí/patchů OS v pravidelných intervalech;
- Změny konfigurací OS;
- Instalace kritických oprav OS;
- Kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;

- Vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu);
- Instalace a konfigurace nového software;
- Instalace a údržba ovladačů a firmware hardware virtualizační platformy;
- Správa účtů v OS;
- Případné úpravy výkonnostních parametrů systému;
- Správa souborového systému (filesystem, přístupová práva, kvóty a limity jeho použití);
- Konzultace při poskytování podpory uživatelům Objednatele a jeho dodavatele aplikace PÚEP;
- Údržba dokumentace o konfiguraci OS;
- Troubleshooting OS;
- Hardening OS;
- Testování změn provedených v OS;
- Komunikace a řešení problémů s externím supportem;
- Konfigurace a nastavení firewallu a antiviru v prostředí OS.

3.3 Poskytování Služby správy databáze

Dále Poskytovatel zajišťuje pro provoz aplikace PÚEP provoz databáze PostgreSQL na samostatném a dedikovaném databázovém serveru a součástí jsou následující provozní činnosti:

- Instalace databázového serveru bez poskytnutí licence;
- Administrace databáze (změny konfigurací databáze, správa účtů v databázi);
- Instalace patchů a kritických oprav;
- Instalace security patchů;
- Upgrade a migrace databáze;
- Definice zálohování a obnovy dat;
- Vyhodnocování výstupů z monitoringu databáze (sledování výkonnostních parametrů a zatížení databáze);
- Úpravy výkonnostních parametrů databáze;
- Reportování výstupů z monitoringu na vyžádání;
- Preventivní údržba databázového serveru a databází;
- Restarty databází dle požadavků Objednatele;
- Odpovídání na technické dotazy Objednateli;
- Údržba dokumentace o konfiguraci databáze;
- Troubleshooting databáze;
- Testování změn provedených v databázi;
- Komunikace a řešení problémů s externím suportem.

3.4 Poskytování dalších provozních služeb

Další součásti Služby jsou následující oblasti, nezbytné pro kompletní provoz Služby dle požadavku Objednatele:

- Příprava, konfigurace a správa síťové infrastruktury, vč. provozního IT monitoringu a logování;
- Poskytnutí konektivity do internetu z DC Poskytovatele s alokovanou kapacitou 50 Mbps vč. nastavení pravidel stavového firewallu a poskytnutí služeb loadbalancingu a SSL terminace;
- Poskytnutí vzdáleného přístupu ke zdrojům výpočetního výkonu prostřednictvím privátní VPN pro celkem 5 uživatelů Objednatele;
- Zajištění konektivity do CMS2 pro přenos dat z poskytovaných serverů do infrastruktury Objednatele;
- Zajištění logování pomocí služby centrálního log managementu, které se provozuje v prostředí Poskytovatele infrastruktury pro sběr, uchování a analýzu logů, které se ze zdrojů logů sbírají pomocí standardních rozhraní. Prostředí je rozděleno do dvou základních vrstev, datová pro sběr, transformaci a ukládání logů, a následně prezentační pro analytickou práci a interpretaci logů nebo událostí dle předpřipravených postupů, filtrů a grafů. Základní přístup do systému lze pro Objednatele poskytnout pro analytické účely v read-only. Připojení jednotlivých zdrojů logů do nástroje log managementu, případně úpravy jejich prezentace nebo reportů potřebných pro provoz řešení, se zajišťuje v součinnosti mezi Objednatelem a Poskytovatelem;
- Příprava, konfigurace a správa zálohování, realizované formou snapshotů image disků jednotlivých serverů;
- Dohled nad kvalitou poskytované služby zahrnuje zejména – vyhodnocování dostupnosti Služby a pravidelný měsíční reporting.

3.5 Příprava Služby

Příprava Služby se skládá z následujících činností:

- Příprava subskripce v prostředí AzS v DC Vápenka
  - Vytvoření a konfigurace jednotlivých zdrojů výpočetního výkonu dle definovaných plánů;
  - Vytvoření a konfigurace síťových prostupů z AzS do prostředí DC Poskytovatele.
- Konfigurační práce na síťové vrstvě
  - Konfigurace síťových prostupů a komunikací na FW;
  - Konfigurace loadbalancerů;
  - Konfigurace klientských VPN přístupů;
  - Konfigurace konektivity do CMS2.
- Příprava OS a databází
  - Instalace operačních systémů MS Windows Server a RHEL na poskytované servery dle požadavku Objednatele;
  - Vytvoření nezbytných účtů v rámci OS a zajištění přístupu pro Objednatele vč. jeho dodavatele;
  - Instalace databázového prostředí PostgreSQL;
  - Vytvoření nezbytných databázových účtů a zajištění přístupu pro Objednatele vč. jeho dodavatele.

3.6 Ostatní

Součástí Služby není instalace, správa či servisní podpora aplikací Objednatele. Poskytovatel pouze zajišťuje nezbytnou součinnost pro Objednatele a jeho dodavatele aplikace PÚEP zejména při zajištění činností vyžadujících administrátorské oprávnění na poskytovaných serverech.

IV.KVALITATIVNÍ PARAMETRY POSKYTOVANÉ SLUŽBY

4.1 Roční dostupnost Služby

Požadavek na roční dostupnost Služby podle tohoto katalogového listu je 99,99 % v každém kalendářním roce. Požadovaná roční dostupnost ve výše uvedených provozních dobách se posuzuje vždy pro aktuální kalendářní rok. Na počátku každého kalendářního roku Poskytovatel vypočítá maximální možné trvání nedostupnosti Služby pro dané období podle uvedených procentuálních hodnot požadované roční dostupnosti.

4.2 Zajištění servisní podpory Služby

Komunikačním kanálem pro hlášení incidentů a požadavků určenými pracovníky Objednatele je Service Desk Poskytovatele (dále jako „Service Desk"). Service Desk je dostupný v režimu 24x7.

ServiceDesk je pracoviště Poskytovatele přijímající servisní hlášení od určených osob Objednatele zadáním požadavku v aplikaci, telefonicky nebo e-mailem. V případě vzniku incidentu, vzniku požadavku na konfigurační úpravu Služby nepřesahující parametrický rámec tohoto katalogového listu a na konzultace ke Službě, jsou k dispozici následující kontakty Poskytovatele:

Aplikace Service Desk – preferovaný způsob (servicedesk.spcss.cz)	[redacted]

Kontakt na pracoviště Service Desku

[redacted]

Service Desk je standardním nástrojem a službou Poskytovatele pro poskytování podpory a řízení provozních procesů. Service Desk je využíván jako prostředek formalizovaného způsobu komunikace s uživateli a pracovníky podpory provozu Objednatele.

Service Desk bude využíván pro předávání informací o provozních incidentech a požadavcích a sledování postupu jejich řešení. Řešitelé incidentů a požadavků budou pracovat přímo v prostředí Service Desk. Poskytovatel je odpovědný za včasný záznam postupu řešení incidentů (v rozsahu jeho odpovědnosti) v Service Desku, v úrovni detailu dostatečné pro spolupráci ostatních účastníků provozu na jejich řešení a pro zpětný audit příčin incidentů a způsobu řešení.

Servisní podpora bude primárně zajišťovaná prostřednictvím pracovníků Poskytovatele nebo jeho dodavatelů na základě smluv uzavřených mezi Poskytovatelem a jeho servisními dodavateli.

Plnění smluvních SLA parametrů Poskytovatele podle tohoto Katalogového listu souvisejících s řešením incidentů bude vyhodnocováno na základě údajů zaznamenaných v Service Desku.

4.3 Odstraňování závad (incident)

Závada je neplánované přerušení nebo zhoršení kvality Služby. Z pohledu závažnosti se závady dělí na následující kategorie:

- Kritická – závada, při níž není Služba použitelná ve svých základních funkcích nebo je zcela nefunkční;
- Závažná – závada, kdy je Služba ve svých funkcích degradovaná natolik, že tento stav omezuje její běžné používání. Dále závada aplikace, která vyžaduje zásah administrátora OS;
- Nezávažná – drobná závada, která nijak významně neovlivňuje Službu.

Požadované lhůty pro Odstranění závady jsou uvedeny v následující tabulce:

Lhůta pro Odstranění závady			
Kategorie závady	**Kritická**	**Závažná**	**Nezávažná**
Popis SLA	7 dnů v týdnu, 24 hodin denně v době od 0:00 do 24:00 hodin, s povinností oznámit zahájení řešení do 30 minut od nahlášení a odstranit závadu do 4 hodin od nahlášení Servisního hlášení.	7 dnů v týdnu, 13 hodin denně v době od 7:00 do 20:00 hodin, s povinností oznámit zahájení řešení do 1 hodiny od nahlášení a odstranit závadu do 8 hodin od nahlášení Servisního hlášení.	5 pracovních dnů v týdnu, 11 hodin denně v době od 7:00 do 18:00 hodin, s povinností oznámit zahájení řešení nejpozději následující pracovní den a odstranit závadu do 55 hodin od nahlášení Servisního hlášení.
Provozní doba (dny)	7 dnů v týdnu	7 dnů v týdnu	5 pracovních dnů v týdnu

Lhůta pro Odstranění závady			
Kategorie závady	**Kritická**	**Závažná**	**Nezávažná**
Provozní doba (hodiny)	nepřetržitě	7:00 – 20:00	7:00 – 18:00
Výjimky z provozní doby	nejsou	nejsou	nejsou
Garantovaný čas reakce operátora	15 minut	30 minut	60 minut
Garantovaný čas zahájení prací na odstranění závady	30 minut	1 hodina	následující pracovní den
Garantovaný čas odstranění závady	4 hodiny	8 hodin	55 hodin

4.4 Řešení provozních požadavků (požadavek)

Požadované lhůty pro Řešení provozních požadavků jsou uvedeny v následující tabulce

Lhůta pro Řešení provozních požadavků	
Popis SLA	5 pracovních dnů v týdnu, 8 hodin denně v době od 8:00 do 16:00 hodin, s povinností oznámit zahájení řešení nejpozději do 2 hodin a vyřešit do 8 hodin.
Provozní doba (dny)	5 pracovních dnů v týdnu
Provozní doba (hodiny)	8:00 – 16:00
Výjimky z provozní doby	Nejsou
Garantovaný čas zahájení řešení požadavku	2 hodiny
Garantovaný čas vyřešení požadavku	8 hodin

4.5 Plánované odstávky

V rámci poskytování Služby si Poskytovatel vyhrazuje právo na plánované odstávky celého nebo částí systému. Nedostupnost Služby v době plánovaných odstávek se nezapočítává do celkové roční nedostupnosti Služby.

Doba odstávky, která byla předem řádně ohlášena se nezapočítává do nedostupnosti Služby. Za ohlášení se považuje informování Objednatele e-mailem na adresu Oprávněné osoby Objednatele a to minimálně 48 hodin před zahájením odstávky. Ovlivnění chodu Služby ze strany Objednatele se nezapočítává do nedostupnosti Služby.

Předpokládaná četnost odstávek je 1x za měsíc, ale může souviset s aktuálním doporučením dodavatele jednotlivých poskytovaných systémů, nebo např. NÚKIB. Předpokládaná doba odstávky je maximálně 1 hodina.

4.6 Definice měření dostupnosti

Dostupnost Služby je definovaná při splnění následující podmínky:

- přenosová trasa je funkční, poskytování Služby není výrazně omezeno, ztíženo nebo přerušeno

Za nahlášení nedostupnosti Služby se považuje založení odpovídajícího servisního hlášení dle postupu uvedeného v kapitole 4.2.

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 \cdot \frac{T - N}{T}$$

kde

D	je dostupnost [%] v daném období
T	vyjadřuje fond provozní doby Služby v daném období
N	vyjadřuje dobu v daném období, kdy byla Služba nedostupná. Do doby nedostupnosti se nezapočítávají plánované odstávky.

- Dostupnost je měřená ročně, a to od 00:00 hod. 1. 1. do 24:00 hod. 31. 12. každého kalendářního roku. Na počátku každého kalendářního roku Poskytovatel vypočítá maximální možné trvání nedostupnosti Služby pro dané období podle uvedených procentuálních hodnot požadované roční dostupnosti.
- Nedostupnost Služby v době schválených plánovaných a mimořádných odstávek se nezapočítává do celkové roční nedostupnosti Služby. Všechny tyto odstávky budou plánovány a následně odsouhlaseny Objednatelem.
- Do doby nedostupnosti se započítávají všechny doby trvání kritických závad včetně neplánovaných odstávek. Pokud byl incident způsoben prokazatelně mimo zodpovědnost Poskytovatele, do doby nedostupnosti se nezapočítává.
- Plánované odstávky jsou, pokud možno, soustředěny do servisních oken, která jsou každý čtvrtek v čase 19:00 až 24:00. Ve výjimečných případech mohou být odstávky Služby oznamovány i mimo tato servisní okna. Ovlivnění chodu Služby ze strany Objednatele se nezapočítává do nedostupnosti Služby.
- Nedostupnost Služby způsobená softwarovou závadou formulářové platformy se nezapočítává do nedostupnosti poskytované Služby.

4.7 Nedodržení kvalitativního parametru Služby

V případě, že ze strany Poskytovatele dojde k nedodržení kvalitativního parametru Služby a pokud se Poskytovatel s Objednatelem nedohodnou jinak, Objednateli vzniká právo na uplatnění smluvní pokuty.

Poskytovatel bude zproštěn povinnosti dodržet kvalitativní parametr Služby, pokud:

- Objednatel prokazatelně neposkytne požadovanou součinnost;
- k nedostupnosti nebo závadě dojde ze strany Objednatele mimo působnost Poskytovatele;
- k nedostupnosti došlo mimo infrastrukturu Poskytovatele;
- vyskytnou se okolnosti, které představují událost vyšší moci.

KATALOGOVÝ LIST č. 02

Název služby	**Bezpečnostní monitoring**

I.OBDOBÍ POSKYTOVÁNÍ SLUŽBY

Služba Bezpečnostní monitoring (dále jen **„Služba KL002"**) je poskytována od termínu milníku, který definuje její zahájení, do termínu ukončení poskytování Služby KL002.

Název milníku	**Termín splnění milníku**
Zahájení poskytování Služby KL002	Na základě Oznámení o zřízení služby bezpečnostního monitoringu
Ukončení poskytování Služby KL002	Na základě ukončení smlouvy

II.REŽIM POSKYTOVÁNÍ SLUŽBY

Služba KL002 bude poskytována v režimu, dle popisu v tabulce:

Režim poskytování Služby KL002	**Doba poskytování Služby KL002**
Standardní provozní doba	Nepřetržitě (24x7)

III.VSTUPY A VÝSTUPY SLUŽBY

3.1 Vstupy

Vstupy dodané Objednatelem pro Službu KL002 jsou:

- Relevantní dokumenty Objednatele;
- Vstupní analýza – zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování odpovídajícího plnění;
- Realizace ověření provozu – zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování plnění.

3.2 Výstupy

Výstupy Služby KL002 jsou:

- Poskytování Služby KL002;
- měsíční zpráva o stavu služby dle tohoto katalogového listu;
- dokumentace Nasazení Služby Bezpečnostního monitoringu v rozsahu uvedeném ve Smlouvě a Proces zvládání kybernetických bezpečnostních incidentů.

IV.POPIS ROZSAHU SLUŽBY

Služba KL002 je ucelené řešení pro pokrytí potřeb bezpečnostní problematiky v souladu s platným právním řádem. Bezpečnostní monitoring je prováděn dohledovým pracovištěm a expertním týmem SOC SPCSS. Služba KL002 je poskytována v nepřetržitém režimu 24x7 a zahrnuje sběr informací, jejich třídění, korelaci, kategorizaci, analýzu a archivaci. Použité technologie a nástroje umožňují detekci známých bezpečnostních útoků, podezřelého chování a anomálií. V rámci Služby KL002 je také poskytován incident management včetně přípravy podkladů pro příslušné orgány v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti (dále také „ZoKB") v platném znění a podle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále také „VoKB"), případně na základě dohody Smluvních stran.

Služba KL002 je rozdělena do čtyř částí. Část 1 je určena k zajištění povinností stanovených příslušnou legislativou, blíže popsáno v kapitole 4.1. Část 2 doplňuje funkcionalitu Služby KL002, nedostupnost jednotlivých součástí Části 2 nemá vliv na poskytování služby v rozsahu Části 1, tedy na zajištění povinností stanovených příslušnou legislativou. Část 1 a Část 2 jsou nedílné součásti Služby KL002.

V Části 3 a 4 jsou obsaženy Doplňkové služby, které jsou nezbytné k zajištění poskytování služby, a to dle požadované architektury, která je určena na základě Vstupní analýzy dle kapitoly 3.1. Doplňkové služby v této části mohou mít vliv na poskytování služby v rozsahu Části 1, tedy na zajištění povinností stanovených příslušnou legislativou.

Část 1 - Součásti Služby Bezpečnostní monitoring povinné k naplnění vybraných opatření (nedílné součásti KL002, poskytováno vždy)	
☒	Sběr logů
☒	Zpracování logů
☒	Monitorování NetFlow
☒	Proces zvládání kybernetických bezpečnostních incidentů (Incident management)
Část 2 - Ostatní součásti Služby Bezpečnostní monitoring (nedílné součásti KL002, poskytováno vždy)	
☒	Uživatelská behaviorální analýza
☒	Přístup do prostředí nástroje SIEM v rozsahu Služby KL002
☒	Zpracování zprávy o stavu Služby KL002 dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu)
Část 3 - Doplňkové služby – Bezpečnostní monitoring databází	
☐	Bezpečnostní monitoring databází
☐	Virtuální kolektor pro Bezpečnostní monitoring databází
☐	Virtuální agregátor pro Bezpečnostní monitoring databází
☐	Virtualizace pro provozování Doplňkových služeb v prostředí SPCSS
☐	Úložný prostor
Část 4 - Doplňkové služby – Bezpečnostní monitoring	
☐	Virtuální kolektor pro Bezpečnostní monitoring
☐	Virtuální procesor pro Bezpečnostní monitoring
☐	Virtualizační prostředí pro provozování služby v prostředí SPCSS
☐	Úložný prostor

Doplňkové služby nejsou součástí základní Služby Bezpečnostní monitoring.

Služba KL002 je realizována v rozsahu definovaných aktiv Objednatele. Archivované informace slouží pro forenzní analýzu ve všech sledovaných souvislostech.

V rámci Služby KL002 je poskytován proces zvládání kybernetických bezpečnostních incidentů (incident management), včetně přípravy podkladů pro hlášení příslušným orgánům. Shromažďované informace jsou na základě požadavku předány pro potřebu interního vyšetřování nebo pro potřeby orgánů činných v trestním řízení.

4.1 Plnění legislativních povinností Objednatele

Služba Bezpečnostní monitoring pokrývá vybrané povinnosti definované zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění, resp. vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti. KL002 obsahuje obecný výčet rozsahu bezpečnostních opatření, které poskytuje Objednateli. Specifika dle klasifikace informací a povahy spravovaného systému (jako KII, VIS) jsou ze strany Objednatele budou určeny požadavkem Objednatele, specifikovány Vstupy dle kapitoly 3.1 a budou zaznamenány v dokumentu „Nasazení Služby Bezpečnostního monitoringu a Proces zvládání kybernetických bezpečnostních incidentů" dle kapitoly 3.2.

Jedná se o tato opatření:

- § 14 Zvládání kybernetických bezpečnostních událostí a incidentů

  Služba KL002 zahrnuje procesy pro detekci a vyhodnocování kybernetických bezpečnostních událostí, zvládání kybernetických bezpečnostních incidentů, ohlašování a posuzování. Služba nabízí nástroje pro klasifikaci, prošetření bezpečnostních událostí včetně návrhu opatření pro odvracení a zmírňování škod.

- § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

  Služba Bezpečnostní monitoring zaznamenává bezpečnostní logy včetně bezpečného uchovávání po dobu požadovanou VoKB (Podmínkou pro splnění tohoto opatření je realizace samostatné Služby Log management SPCSS, která není předmětem tohoto KL002, nebo využití odpovídajících Doplňkových služeb specifikovaných na základě Vstupní analýzy dle kapitoly 3.1).

- § 23 Detekce kybernetických bezpečnostních událostí

  Služba KL002 disponuje nástroji pro detekci kybernetických bezpečnostních událostí, ověřováním a kontrolou přenášených dat v komunikačních sítí a na jejím perimetru.

  Při ochraně prostředí Objednatele umožňuje s ohledem na důležitost aktiv zajistit detekci kybernetických bezpečnostních událostí v rámci koncových stanic, mobilních zařízení, serverů, datových úložišť a výměnných datových nosičů, síťových aktivních prvků a obdobných aktiv.

- § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí

  V prostředí Objednatele lze Službu KL002 využít pro sběr bezpečnostních událostí a jejich vyhodnocování. Služba KL002 poskytuje informace určeným bezpečnostním rolím v organizaci, čímž omezuje případy nesprávného vyhodnocení události a zajišťuje včasné varování.

- § 31 Kategorizace kybernetických bezpečnostních incidentů

Služba KL002 umožňuje kategorizovat jednotlivé bezpečnostní incidenty dle významnosti. Bezpečnostní incidenty lze kategorizovat dle dopadových kritérií, počtu dotčených uživatelů, škod způsobených nebo předpokládaných. Kategorizovat lze také podle dopadu na služby nebo délkou trvání incidentu.

- § 32 Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

  Služba Bezpečností monitoring zajišťuje přípravu podkladů, vytvoření hlášení o kybernetickém bezpečnostním incidentu. Po zajištění všech potřebných informací provede nahlášení patřičným způsobem a formou příslušným orgánům.

Služba KL002 nezahrnuje organizační opatření SŘBI Objednatele. Součástí Služby KL002 není tvorba politik, vyjma dokumentace dle kapitoly 3 tohoto katalogového listu.

V.POPIS JEDNOTLIVÝCH ČÁSTÍ SLUŽBY KL002

Předmětem Služby KL002 je nepřetržitý bezpečnostní monitoring v režimu 24x7 definovaných aktiv Objednatele.

Typy záznamů, se kterými Služba KL002 pracuje, jsou zejména:

- logy operačních systémů;
- logy aplikací;
- logy síťových prvků;
- logy infrastruktury a virtualizačního prostředí;
- NetFlow.

5.1 Zpracování logů

Služba je poskytována za využití nástrojů a prostředků ve vlastnictví SPCSS, které zprostředkovávají realizaci sběru, vyhodnocování a uchovávání logů.

Zpracování logů má významnou funkci nejen pro analýzu obsažených informací, ale i pro ochranu před ztrátou, poškozením nebo úmyslnou modifikací těchto záznamů. Ze systémových logů lze čerpat celou řadu informací, např.: přihlášení uživatele, informace o uživatelských aktivitách, záznam o konfiguračních změnách systému a jiné. Získané informace lze využít k detekci anomálií chování uživatelů, infrastruktury nebo samotných aplikací.

Dalším opatřením, které stanovuje VoKB je ukládání získaných informací – logů, v bezpečném úložišti, které zajišťuje ochranu proti změnám nebo smazání. Logy získané z monitorovaných aktiv Objednatele je nezbytné uchovávat po dobu stanovenou VoKB pro příslušný typ systému. Uchování logů po dobu delší, než ukládá VoKB a současně vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu pro BÚ 4, není součástí služby KL002. Podmínkou pro splnění tohoto opatření je realizace samostatné Služby Log management SPCSS, která není předmětem tohoto KL002 nebo dle dohody mezi smluvními stranami.

5.2 Monitorování NetFlow

Tato služba obsahuje monitorování síťového provozu na základě datových toků na síťové vrstvě. Tento způsob monitorování poskytuje podrobný pohled do provozu na síti v reálném čase. S pomocí NetFlow statistik lze odhalovat vnější i vnitřní incidenty, sledovat zdroje a cíle komunikace, jak dlouho, pomocí jakého protokolu a kolik bylo přeneseno dat. Monitorování NetFlow důrazně doporučujeme s ohledem na kontext vyhodnocování událostí z monitorovaných systémů. Informace

o NetFlow výrazně zvýší přehled o dění v monitorovaných systémech a dokáže odhalit například podezřele dlouhé, nebo objemné přenosy dat nejen do internetu, ale i v rámci infrastruktury Objednatele nebo komunikaci s IP adresami s nízkou reputací (rozesílání, malware, spamu, skenování atd.). Pro monitoring NetFlow v prostředí Objednatele je doporučena instalace NetFlow kolektoru (jedná se o službu Virtuální kolektor pro bezpečnostní monitoring) z důvodu úspory kapacity datového toku a zaručení dodávky dat do SIEM.

Integrace, konfigurace a správa NetFlow kolektoru není součástí základní Služby KL002.

Dodávka NetFlow kolektoru je řešena jako doplňková služba Virtuální kolektor pro bezpečnostní monitoring. Doporučení pro využití NetFlow kolektoru (Virtuální kolektor pro bezpečnostní monitoring) je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

5.3 Uživatelská behaviorální analýza

Služba obsahuje analýzu chování uživatelů *(User behavior analytics – UBA).* Technologie analyzuje aktivitu uživatelů a zjišťuje, zda došlo ke zneužití účtu uživatele. UBA přidává kontext uživatele k síti, protokolu, zranitelnostem a ohrožení dat rychleji a přesněji detekuje útoky. Bezpečnostní analytici mohou snadno zobrazit rizikové uživatele, zobrazit jejich anomální aktivity a zkoumat konkrétní podkladové protokoly, logy a toky dat, která přispěla k hodnocení rizika uživatele.

5.4 Přístup do prostředí nástroje SIEM v rozsahu Služby KL002

V rámci služby je určeným pracovníkům Objednatele umožněn přístup do prostředí SIEM, kde mohou sledovat aktivity, které generují monitorované systémy. Objednatel si může nastavit vlastní přehledové obrazovky a grafy, sledovat Offense nebo výpisy z logů, které jsou zpracovány nástrojem SIEM. Objednatel má přístup pouze k informacím v rozsahu svých systémů.

Prostředí zpřístupněné Objednateli (tzv. tenant) je vyhrazené prostředí, které vidí pouze daný Objednatel. Data jsou zpracovávána a ukládána v daném prostředí tenanta.

Toto prostředí slouží pouze jako přehledové s možností dohledávání historických dat. Náhled neslouží pro vyšetřování KBU, KBI ani pro analýzy.

Při nasazení služby proběhne školení určených pracovníků Objednatele. Toto školení bude realizováno dle požadavku Objednatele, nejméně jednou za rok.

Maximální počet pracovníků Objednatele, kteří budou moci využívat přístup do prostředí SIEM, je stanoven na 10 pracovníků.

Nedostupnost tohoto prostředí Objednateli nemá vliv na řešení KBU/KBI ze strany Poskytovatele, neovlivňuje dostupnost a kvalitu poskytované služby bezpečnostního monitoringu a nemá tak vliv na plnění SLA; více v kapitole 6 tohoto katalogového listu.

5.5 Incident management – proces zvládání kybernetických bezpečnostních incidentů

Incident response je aplikován na zvládání všech zjištěných nebo hlášených událostí a incidentů. Expertní týmy aktivně řeší události od počátku až po jeho vyřešení a uzavření. Aktivita týmů zahrnuje vyhodnocování, zvládání, dokumentování Bezpečnostních Hlášení *(BH),* Kybernetických Bezpečnostních událostí *(KBU)* a Kybernetických Bezpečnostních incidentů *(KBI).* Nedílnou součástí je analýza a návrh na zlepšování bezpečnosti Informačních Systémů *(IS)* ve sledovaném prostředí. Primárním subjektem odpovědným za řešení a zvládání událostí a incidentů je CSIRT–SPCSS.

Monitoring a detekce KBU a KBI v režimu 24x7 je zajištěna dohledovým pracovištěm SPCSS, nástrojem SIEM a expertním týmem Security Operation Center (dále také jen „SOC"). Nástroj SIEM v reálném čas monitoruje a vyhodnocuje probíhající události na sledovaných aktivech a na základě implementovaných pravidel automaticky sestavuje bezpečnostní výstrahy, které nesou informace o narušení bezpečnostního stavu. Tato funkcionalita je zajištěna sběrem událostí v nástroji SIEM

z vybraných zdrojů logů, které jsou definovány na základě podkladů od Objednatele, resp. na základě analýzy rizik.

Řízení incidentů je vedeno pomocí systému podchycujícího jednotlivé kroky odborníků, vyšetřujících detekované nebo hlášené události *(Incident Response Platform).* Tento nástroj pomáhá od počátku až do finálního vyřešení požadavku. Velký význam nástroje je v jeho specifické funkcionalitě, která agreguje bezpečnostní informace z rozdílných zdrojů na jednom místě. Toto propojení informací na jednom místě pomáhá při řešení sofistikovaných útoků, jejichž počet v poslední době narůstá. Jedním ze zdrojů je otevřená platforma pro sdílení informací o hrozbách, které jsou aktualizovány v celosvětovém měřítku *(Threat Intelligence Platform).*

Nezbytným pro činnost CSIRT-SPCSS při provádění evidence a vyhodnocování událostí je aplikace Service Desk. Jedná se o jednotné prostředí pro řízení procesu Incident response. V aplikaci je prováděna evidence stavu i jednotlivé kroky řešení události. Systém umožňuje sledovat průběh události, ale i následné řešení. Podklady zpracovávané v systému Service Desk slouží k řešení a vyhodnocování bezpečnostních hlášení, kybernetických bezpečnostních událostí nebo kybernetických bezpečnostních incidentů. Zdroje pro vyhodnocované události mohou pocházet od uživatelů, bezpečnostních specialistů, administrátorů nebo pomocí technických prostředků.

Service Desk je prostředí obsahující informace, které slouží jako podklad pro expertní tým OCKB – SOC při zvládání kybernetických bezpečnostních událostí a bezpečnostních incidentů. Definovanými procesy v prostředí Service Desk jsou uzpůsobeny pro zvládání KBU a KBI a následné řízení změn.

Aktivity CSIRT-SPCSS poskytované v rámci služby pro zvládání kybernetických bezpečnostních incidentů:

- zabezpečení procesu zvládání BH, KBU, KBI;
- detekci KBU, KBI;
- klasifikaci KBU, KBI;
- zpracování dokumentace KBU a KBI včetně uchovávání relevantních dat v nástroji SIEM (logů, událostí, „offense"…), vedení záznamů v Service Desk (systém zákaznické podpory, dále jen SD) o průběhu řešení, zavedení a aktualizace znalostní báze v SD;
- iniciaci bezpečnostních varování a opatření včasné reakce v případech velmi závažných a závažných KBI;
- zajištění realizace reaktivních opatření NÚKIB;
- příprava proaktivních opatření obrany v závislosti na rozvoj hrozeb;
- přípravu podkladů pro informování příslušných orgánů.

5.6 Pravidelná zpráva o stavu služby dle tohoto katalogového listu

Zpráva obsahuje tyto informace:

- Období poskytování Služby KL002;
- Režim poskytování Služby KL002;
- Popis rozsahu Služby KL002;
- Monitorovaná prostředí;
- Rozsah bezpečnostního dohledu;
- Detekce, sběr a vyhodnocování kybernetických bezpečnostních událostí;
- Stav dokumentace (aktualizace dokumentace dle kapitoly 3.2);

- Řízení provozu služeb;
- Řešení a stav BH *(Bezpečnostní hlášení)*, KBU, KBI za uplynulé období a návrhy na nápravná opatření;
- Aktivity Služeb Bezpečnostního dohledu – seznam řešených offense;
- TOP 10 kategorií uplatněných pravidel na firewallu směrem z internetu;
- TOP 10 druhů komunikace zablokovaných z internetu;
- TOP 10 zablokovaných IP adres;
- TOP 10 cílových portů, na které byla zablokovaná komunikace;
- TOP 10 zablokovaných aktivit na firewallu;
- Návrh na nápravná opatření.

VI.SLA PARAMETRY

Poskytovatel je povinen poskytovat Službu KL002 dle Smlouvy pro vybrané aktiva Objednatele v souladu s jednotlivými níže uvedenými kvalitativními parametry Služby pro její jednotlivé části.

Ovlivnění chodu všech částí Služby KL002 ze strany Objednatele (přerušení zasílání logů úplné nebo částečné a obdobné) a z důvodů mimo působnost Poskytovatele se nezapočítává do nedostupnosti žádné z částí Služby KL002.

6.1 Požadovaná měsíční dostupnost částí služby – Vybraná část Části 1, ČÁST 3 a ČÁST 4

Název Služby:	**Bezpečnostní monitoring**	
SLA parametry		
Část Služby:	**Dostupnost Služby:**	**Servisní okno pro odstávky:**
Část 1 - Sběr logů, zpracování logů, Monitoring Netflow v nástroji SIEM	99,99 %	každý čtvrtek, vždy 19:00-24:00
Část 3 – Doplňková služba – Bezpečnostní monitoring databází, Virtuální kolektor pro Bezpečnostní monitoring databází, Virtuální agregátor pro Bezpečnostní monitoring databází	99,99 %	každý čtvrtek, vždy 19:00-24:00
Část 4 – Doplňková služba – Virtuální kolektor pro Bezpečnostní monitoring, Virtuální procesor pro Bezpečnostní monitoring,	99,99 %	každý čtvrtek, vždy 19:00-24:00

Tabulka – Požadovaná měsíční dostupnost částí služby – vybraná část Části 1, Část 3 a Část 4

Nedostupnost Služby KL002 – Část 1 (Sběr logů, zpracování logů, Monitoring Netflow v nástroji SIEM), Část 3 (Bezpečnostní monitoring databází, Virtuální kolektor pro Bezpečnostní monitoring databází, Virtuální agregátor pro Bezpečnostní monitoring databází) Část 4 (Virtuální kolektor pro Bezpečnostní monitoring, Virtuální procesor pro Bezpečnostní monitoring,) způsobená hardwarovou nebo jinou technickou závadou se počítá od okamžiku zahájení nedostupnosti Služby KL002 – Část 1, Část 3 a Část 4 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL002 – Část 1, Část 3 a Část 4 ve výše definovaném rozsahu, počítá se nedostupnost služby od doby jejího nahlášení.

Za nahlášení nedostupnosti služby se považuje založení odpovídajícího servisního hlášení v aplikaci Service Desk SPCSS (servicedesk.spcss.cz).

Nedostupnost součástí Služby KL002 – Část 2 - Uživatelská behaviorální analýza, Přístup do prostředí nástroje SIEM v rozsahu Služby KL002, Zpracování zprávy o stavu Služby KL002 dle tohoto katalogového listu určené Objednateli (předávána v měsíčním intervalu) - neovlivňuje dostupnost a kvalitu poskytované Služby KL002 – Část 1, Část 3 a Část 4 ve výše definovaném rozsahu a nemá tak vliv na plnění příslušného SLA.

6.1.1 Postup výpočtu dostupnosti Služby

Dostupnost služby se vypočítá podle následujícího vzorce:

$$D = 100 * \frac{T - N}{T}$$

kde:

D	je dostupnost [%] v daném období
T	vyjadřuje fond provozní doby služby v daném období
N	vyjadřuje dobu v daném období, kdy byla služba nedostupná. Do doby nedostupnosti se nezapočítávají pravidelné odstávky, mimořádné odstávky a další specifické Části Služby KL002.

6.1.2 POŽADOVANÉ LHŮTY PRO OBNOVENÍ SLUŽBY KL002 – VYBRANÁ ČÁST ČÁSTI 1, ČÁST 3 A ČÁST 4

Název Služby:	**Bezpečnostní monitoring**		
Část Služby:	**Lhůta pro obnovení služby v běžné provozní době v hodinách**		
	Incident kategorie A	**Incident kategorie B**	**Incident kategorie C**
Část 1 – Sběr logů, zpracování logů, Monitoring Netflow v nástroji SIEM	4	24	168
Část 3 - Bezpečnostní monitoring databází, Virtuální kolektor pro Bezpečnostní monitoring	4	24	168

databází, Virtuální agregátor pro Bezpečnostní monitoring databází			
Část 4 - Virtuální kolektor pro Bezpečnostní monitoring, Virtuální procesor pro Bezpečnostní monitoring	4	24	168

Tabulka – Požadované lhůty pro obnovení Služby KL002 – vybraná část Části 1, Část 3 a Část 4

Kategorizace provozních incidentů:	
Incident kategorie A	Služba není dostupná ve svých základních a klíčových funkcíc, a přitom tato funkční závada znemožňuje její užívání. Tento stav kritickým způsobem omezuje běžný provoz.
Incident kategorie B	Služba je ve svých funkcích degradována tak, že tento stav zásadně omezuje (Nefunkční dílčí součást v rozsahu vybrané součásti Části 1 a Část 3) její běžný provoz.
Incident kategorie C	Ostatní incidenty, které nespadají do kategorií A nebo B.

Tabulka – Kategorizace provozních incidentů

6.2 Reakční doby a doby odstranění kybernetického bezpečnostního incidentu Služby KL002 – Část 1

Doba reakce úrovně L1 je počítána od zaevidování offense/bezpečnostního hlášení/kybernetické bezpečnostní události/kybernetického bezpečnostního incidentu (BH/KBU/KBI) do aplikace Service Desk SPCSS (servicedesk.spcss.cz). Podpora L1 musí do doby uvedené v tabulce níže přijmout v aplikaci Service Desk BH/KBU/KBI k řešení.

Název Služby:	**Bezpečnostní monitoring**		
Část Služby:	**Maximální doba zahájení řešení incidentu v pracovní dny 6–18 hod.**	**Maximální doba zahájení řešení incidentu v mimopracovní dny a v době 18–6 hod.**	**Doba odstranění incidentu**
Část 1 – Proces zvládání kybernetických bezpečnostních incidentů (Incident management)	15 minut	30 minut	Po dohodě obou smluvních stran

Tabulka – Reakční doby a doby odstranění incidentu

6.3 Požadovaná měsíční dostupnost části služby – Část 2 - Přístup do prostředí nástroje SIEM v rozsahu Služby KL002

Název Služby:	**Bezpečnostní monitoring**	
SLA parametry		
Část Služby:	**Dostupnost Služby:**	**Servisní okno pro odstávky:**
Část 2 – Přístup do prostředí nástroje SIEM v rozsahu Služby KL002	95 %	každý čtvrtek, vždy 19:00-24:00

Tabulka – Přístup do prostředí nástroje SIEM v rozsahu Služby KL002

Nedostupnost Služby KL002 – Část 2 (Přístup do prostředí nástroje SIEM v rozsahu Služby KL002) způsobená hardwarovou nebo jinou technickou závadou se počítá od okamžiku zahájení nedostupnosti Služby KL002 – Část 2 ve výše definovaném rozsahu do okamžiku obnovení poskytování. V případě, že není možné prokazatelně zjistit okamžik zahájení nedostupnosti Služby KL002 – Část 2 ve výše definovaném rozsahu, počítá se nedostupnost služby od doby jejího nahlášení.

Za nahlášení nedostupnosti služby se považuje založení odpovídajícího servisního hlášení v aplikaci Service Desk SPCSS (servicedesk.spcss.cz).

Lhůta pro obnovení služby v běžné provozní době v hodinách je stanovena dle incidentu Kategorie C dle kapitoly 6.1.2 tohoto Katalogového listu.

Ovlivnění chodu částí Služby KL002 Část 2 – Přístup do prostředí nástroje SIEM v rozsahu Služby KL002 ze strany Objednatele (přerušení komunikace na straně Objednatele, a to úplné nebo částečné a obdobné) se nezapočítává do nedostupnosti žádné z částí Služby KL002 Část 2 – Přístup do prostředí nástroje SIEM v rozsahu Služby KL002.

6.4 Plánované odstávky

V rámci poskytování Služby KL002 si Poskytovatel vyhrazuje právo na plánované odstávky celého nebo částí systému z důvodu údržby jak samotného systému, tak infrastruktury a datové konektivity Poskytovatele. Poskytovatel se zavazuje plánované práce s vlivem na dostupnost Služby KL002 soustředit do jednoho termínu tak, aby byla poskytovaná Služba KL002 ovlivněna co nejméně.

Plánované odstávky jsou, pokud možno, soustředěny do servisních oken, která jsou každý čtvrtek v čase 19:00 až 24:00. Ve výjimečných případech jsou odstávky Služby KL002 ohlašovány a realizovány i mimo tato servisní okna. Doba odstávky, která byla předem řádně ohlášena se nezapočítává do nedostupnosti Služby KL002. Za ohlášení se považuje informování určených osob Objednatele e-mailem, a to minimálně 24 h před zahájením mimořádné odstávky.

VII.DOPLŇKOVÉ SLUŽBY

Doplňkové služby nemohou být poskytovány samostatně. Podmínkou pro poskytování doplňkových služeb je využití hlavní služby Bezpečnostní monitoring, respektive službu Bezpečnostní monitoring databází, dle povahy řešení. Režim poskytování doplňkových služeb je v souladu s kapitolou 2 a kapitolou 6 tohoto katalogového listu.

7.1 Bezpečnostní monitoring databází

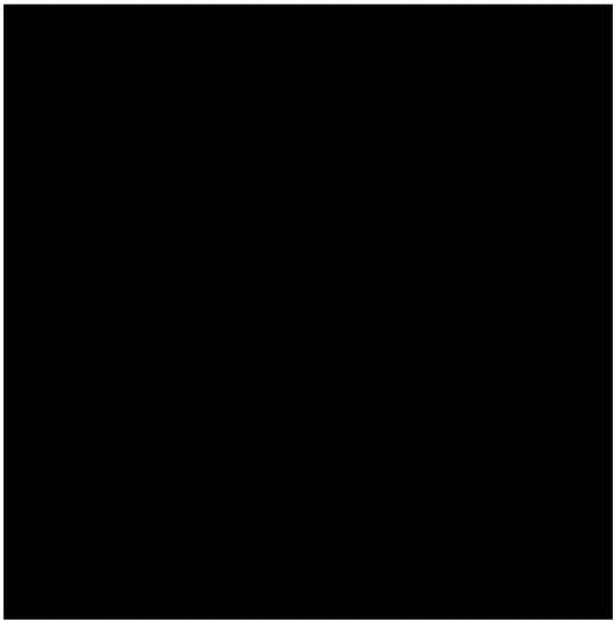
Doplňková služba Bezpečnostní monitoring databází pomáhá se zabezpečením citlivých dat v prostředí databází a datových skladů. Bezpečnostní monitoring databází se skládá ze dvou částí – kolektor *(jedná se o kolektor speciálně určený pro monitoring databází)* a nástroj pro analýzu a ochranu dat v databázích. Pro integraci služby je zapotřebí využít obě položky.

Systém umožňuje chránit strukturovaná i nestrukturovaná data. Monitoruje a vyhodnocuje činnosti uživatelů databáze a databázových administrátorů. Služba umožňuje chránit data s ohledem na platná pravidla a nařízení, nabízí kontrolu nad tím, jak je s informacemi zacházeno. Služba pomáhá v pokrytí požadavků v oblastech definovaných legislativou. Rozsah funkcionalit služby se pohybuje v rozsahu od obecných hrozeb až po nesplnění náplně regulačních auditů. Architektura služby je škálovatelná. Služba se skládá vždy ze dvou položek: systému pro obranu databází a kolektoru. Kolektor agreguje a zpracovává data až ze šesti databázových serverů.

Služba dokáže porozumět všem transakcím, ve všech protokolech, na celé řadě platforem. Služba pomáhá v situacích, kdy se rozsah dat mění dynamicky a data jsou distribuovaná v různých místech.

V takto komplexních situacích je využití běžných logovacích mechanismů, které jsou součástí vlastních systémů, velmi komplikované a nedostatečné. Běžné logovací mechanismy také nemají nástroje pro zajištění důvěrnosti logovaných informací. Výsledkem využití služby monitoringu databází je komplexní pohled na informace o využívání dat, přehled chování uživatelů a kontrola pravidel přístupu k informacím v celkovém kontextu sledovaného systému.

Pokud se jedná o neautorizované změny informací z uživatelských účtů, dokáže systém identifikovat autora změn. Informace o aktivitách uživatelů jsou vytvářeny nezávisle na logovacích a auditních funkcích databáze jako takové. Pomocí služby lze sledovat i vynucovat bezpečnostní pravidla pro přístup k citlivým datům *(informace typu PII, PCI atd.)*.



Pro testování ohrožení a zjišťování rizik využívá služba automatizované klasifikační techniky nové generace na bázi kognitivní analýzy. Služba využívá informace, které získává analýzou z pravidelného chování uživatele, a je tak schopna zabránit aktivitám, které nejsou popsány pravidly – např. může se jednat o skenování a vytěžování dat v případě pokusu o odcizení. Systém je schopen v reálném čase detekovat, předávat notifikace, ale i ochránit data.

Služba je schopna generovat výstupy pro potřeby auditu z celé sledované oblasti. Zajištěná auditní stopa, kterou služba poskytne, je chráněna proti nedovolené manipulaci a obsahuje informace požadované auditory.

Pomocí služby Bezpečnostní monitoring databází lze monitorovat a chránit databáze a datové sklady provozované na Windows, UNIX, Linux, AS/400.

Doporučení pro využití služby Bezpečnostního monitoringu databází v rámci architektury řešení poskytované Služby KL002 je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

7.2 Virtuální kolektor pro Bezpečnostní monitoring databází

Doplňková služba Virtuální kolektor je nedílnou součástí při využití Bezpečnostního monitoringu databází. Kolektor provádí nasazení zásad ochrany informací, provádí procesy auditu. Dále sbírá, analyzuje, a loguje aktivity databází v reálném čase. Služby virtuálního kolektoru slouží pro okamžité

zasílání alertů, ale i pro následnou analýzu. Tento kolektor umí zpracovávat informace z více databázových serverů. Počet napojených serverů, je závislý na celé řadě parametrů, jejichž prověření je předmětem *Vstupní analýzy*. Dle rozsahu infrastruktury je možné implementovat více kolektorů pro Bezpečnostní monitoring databází. Virtuální kolektor pro bezpečnostní monitoring databází lze provozovat v režimu vysoké dostupnosti. Kolektor je umísťován co nejblíže zdroji/databázím v prostředí Objednatele (virtualizace). Výrobcem je definován maximální počet databázových serverů, které lze připojit na jeden kolektor.

Požadovaný rozsah zdrojů virtualizace (vCPU, vRAM, HDD) je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Doporučení pro využití Virtuálního kolektoru databází v rámci architektury řešení poskytované Služby KL002 je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

7.3 Virtuální agregátor pro Bezpečnostní monitoring databází

Doplňková služba Virtuální agregátor konsoliduje data z kolektorů a zároveň poskytuje možnosti uchovávání a správu dat. Toto řešení je primárně určeno pro centrální správu všech instancí Bezpečnostního monitoringu databází, které jsou na něj připojeny.

Virtuální agregátor je umísťován co nejblíže zdroji informací v prostředí Objednatele nebo v prostředí SPCSS NDC, a to v případě, že je definované aktivum Objednatele provozováno v prostředí NDC. Výrobcem je definován maximální počet kolektorů, které lze připojit na jeden agregátor.

Požadovaný rozsah zdrojů virtualizace (vCPU, vRAM, HDD) je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Pokud je implementován Virtuální agregátor v prostředí SPCSS NDC, je cena za poskytované prostředky virtualizace (vCPU, vRAM, HDD – Doplňkové služby Virtualizace pro provozování Doplňkových služeb v prostředí SPCSS, Úložný prostor) kalkulována samostatně. Rozsah potřebných prostředků je závislý na velikosti monitorovaného prostředí.

Doporučení pro využití a umístění Virtuálního agregátoru databází v rámci architektury řešení poskytované Služby KL002 je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

7.4 Virtuální kolektor pro Bezpečnostní monitoring

Nejedná se o doplněk ke službě Bezpečnostní monitoring databází, služba Bezpečnostní monitoring databází má vlastní kolektor.

Doplňková služba Virtuální kolektor pro bezpečnostní monitoring je určena pro monitorované aktivum Objednatele, které je z pohledu architektury sítě mimo prostředí SPCSS. Kolektor je umístěn do síťového prostředí, kde se nachází monitorovaný systém. Tento kolektor je appliance umístěná ve virtualizačním prostředí. Kolektor slouží k zabezpečenému (šifrovanému) a zaručenému (potvrzovanému) přenosu logů do nástroje SIEM, a to i v případě, že je spojení mezi kolektorem a nástrojem SIEM přerušeno. V době přerušení spojení kolektor ukládá logy do mezipaměti. V okamžiku obnovení spojení se logy z mezipaměti odešlou do nástroje SIEM. Kolektor má tři módy odesílání logů:

- Odesílání logů v reálném čase;
- Odesílání logů dávkově;

- Řízení šířky pásma při odesílání logů.

Virtuální kolektor je umísťován co nejblíže zdroji informací v prostředí Objednatele (virtualizace).

Požadovaný rozsah zdrojů virtualizace (vCPU, vRAM, HDD) je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Doporučení pro využití a umístění Virtuálního kolektoru pro bezpečnostní monitoring v rámci architektury řešení poskytované Služby KL002 je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

7.5 Virtuální procesor pro Bezpečnostní monitoring

Doplňková služba Virtuální procesor zpracovává a analyzuje události, které získává z jednoho nebo více kolektorů. Každý procesor má lokální úložiště, data událostí jsou tedy uložena v procesoru, ale je možné data ukládat i mimo do datového nodu. Virtuální procesor pro bezpečnostní monitoring může být implementován jak v prostředí Objednatele, tak v prostředí SPCSS NDC.

Požadovaný rozsah zdrojů virtualizace (vCPU, vRAM, HDD) je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Pokud je implementován Virtuální procesor pro bezpečnostní monitoring v prostředí SPCSS NDC, je cena za poskytované prostředky virtualizace (vCPU, vRAM, HDD – Doplňkové služby Virtualizace pro provozování Doplňkových služeb v prostředí SPCSS, Úložný prostor) kalkulována samostatně. Rozsah potřebných prostředků je závislý na velikosti monitorovaného prostředí.

Doporučení pro využití a umístění Virtuálního procesoru v rámci architektury řešení poskytované Služby KL002 je stanoveno na základě Vstupní analýzy dle kapitoly 3.1.

7.6 Virtualizační prostředí pro provozování služby v prostředí SPCSS

Doplňková služba slouží k zajištění a provozování virtualizovaného prostředí Služby KL02 v případě realizace v prostředí SPCSS NDC.

Požadovaný rozsah zdrojů virtualizace je specifikován na základě Vstupní analýzy dle kapitoly 3.1.

Standardem je platforma x86, 64bit. Virtualizační platforma je provozována na technologii VMware v minimální verzi VMware vSphere 6.7. Součástí služby jsou SW licence virtualizační platformy a aktualizace verzí virtualizačního SW. Na úrovni virtualizace jsou fyzické core mapovány na virtuální CPU (vCPU). Poměr agregace vCPU 10:1 core a zajištění alokace výkonu 1 vCPU odpovídajícího výkonu 1 fyzického core je realizováno prostředky VMware a je v odpovědnosti Dodavatele. Mapování RAM: vRAM je 1:1.

Prostředí se skládá z těchto jednotek:

7.6.1 Building block

Základní stavební jednotkou je Building block (dále také „BB"). Pro provoz virtuálních systémů UNIX/Linux je stanoven BB s poměrem 1:2 (1 vCPU + 2 GB vRAM).

7.6.2 UNIX / LINUX/Linux Critical, Unix-Linux High

Správa operačních systémů různých typů (Unix, Linux) včetně využití externí L3 podpory operačních systémů.

- Dostupnost (roční): 99,9 % pro OS umístěné na replikovaných BB. 99,5 % pro OS umístěné na nereplikovaných BB
- Provozní doba: 24x7 pro Critical, 11x5 pro High

Jednotka obsahuje správu operačních systémů na úrovni fyzických i virtuálních serverů. Administrátorské účty OS jsou v rukou Dodavatele. Objednatel používá pro implementaci a podporu provozu aplikací uživatelské účty, využití administrátorských účtů je možné pouze se součinností Dodavatele nebo bezpečným mechanismem schváleným Dodavatelem.

Služba zahrnuje následující činnosti:

- Administrace operačních systémů;
- Aktualizace operačních systémů (instalace patchů a security patchů) na základě doporučení výrobce, požadavků Objednatele a s ohledem na stabilitu provozu aplikací;
- Kontrola existence bezpečnostních patchů OS a analýza jejich dopadů na provoz;
- Provádění restartů operačních systémů dle požadavků Objednatele;
- Změny konfigurací OS;
- Vyhodnocování výstupů z monitoringu a reportování výkonů a zatížení (expertní konzultační práce nad výstupy, které jsou součástí běžného provozu);
- Profylaxe systému dle harmonogramu v měsíčních intervalech;
- Součinnosti s případnou instalací a konfigurací nového software;
- Instalace a údržba ovladačů a firmware hardwaru;
- Instalace a údržba certifikátů doporučených dodavatelem aplikace pro zabezpečení přístupů na servery;
- Správa lokálních uživatelských účtů v OS;
- Úpravy výkonnostních parametrů systému;
- Správa souborového systému (filesystem, přístupová práva a naplněnost);
- Komunikace a řešení problémů s externí L3 podporou;

Předpokladem poskytování služeb je splnění následujících pravidel:

- Účty s administrátorskými právy jsou v rukách Dodavatele. Použité vyšších práv uživatelským nebo aplikačním účtům Objednatele probíhá formou nástrojů typu sudo nebo pod dohledem pracovníků Dodavatele a ve všech případech podléhá schválení ze strany Dodavatele;
- Aplikační adresáře s rostoucím objeme dat (logy, databáze, úložiště souborů) jsou umístěny na samostatných diskových prostorech (volume, logický disk);

7.6.3 Replikované jednotky

Replikované varianty jednotek zajišťují vysokou dostupnost prostředky virtualizační platformy. Ke každému BB je alokován záložní BB ve druhém DC. V případě výpadku zdrojů v jednom DC dojde k obnovení provozu v druhém DC. Replikace se provádí na úrovni virtuálních serverů (tj. všechny BB jednoho virtuálního serveru musí být replikované) a předpokladem je rovněž zdvojená konfigurace všech diskových prostorů STOR1 nebo STOR3 daného virtuálního serveru. Replikace diskových prostorů do druhého DC se provádí prostředky virtualizace a je asynchronní.

Virtualizované bloky výpočetního výkonu je možno použít ve všech bezpečnostních zónách včetně DMZ.

7.6.4 Unix/Linux server startup rundown

Jednotka zahrnuje služby spojené s instalací nebo s ukončením provozu operačního systému. Provozní doba:11x5

Jednotka přípravy infrastruktury OS zahrnuje zejména následující činnosti:

- Prvotní instalace OS;
- Připojení a konfigurace sítí a diskových prostorů;
- Prvotní konfigurace OS dle požadavků aplikace;
- Instalace bezpečnostních záplat, rozšíření a balíčků;
- Zavedení do konfiguračních databází, provozního a bezpečnostního dohledu, úpravy dokumentace infrastruktury.

Jednotka ukončení infrastruktury OS zahrnuje zejména následující činnosti:

- Zrušení/odinstalace virtuálního serveru;
- Zrušení konfigurace sítí a diskových prostorů;
- Smazání z konfiguračních databází, provozního a bezpečnostního dohledu, úpravy dokumentace infrastruktury;
- Předání nebo migrace dat z rušeného serveru.

7.7 Úložný prostor

Úložný prostor je realizován na diskových polích s primárně točivými disky v kombinaci s Flash disky.

Název využívaných jednotek je STOR1 a STOR3.

7.7.1 STOR1

Je služba realizována na diskových polích s primárně točivými disky v kombinaci s Flash disky (cca 10-20 % objemu). Nad oběma druhy datových úložišť pracuje auto-tiering, který se stará o to, aby nejvytěžovanější bloky dat byly umístěny na Flash mediích a byl tak výrazně navýšen reálný výkon úložiště.

7.7.2 STOR3

Je služba realizována točivými disky (600 GB/10k SAS 2,5") organizovanými do RAID-5. STOR3 není vhodný pro více zatížené transakční databáze.

Služby poskytování diskového prostoru zahrnují zejména následující činnosti:

- prvotní zajištění a instalaci HW a firmware diskových polí a SAN;
- konfigurace diskových jednotek a portů, konfigurace a správa RAIDů, tiering, zoningu;
- správu a konfiguraci storage zařízení;
- posouzení vlivu na všechny zákazníky sdílených platforem;
- proaktivní monitoring HW a řešení incidentů;
- preventivní systémovou údržbu;
- aktualizace firmware storage zařízení. (controllery, disky atd) na základě doporučení výrobce a s ohledem na stabilitu provozu;
- konfigurace a správa SAN protokolů a SAN prvků (optika Fibre Channel);
- vytváření a úpravu LUNů a Volumů a jejich mapování pro servery;

- konfigurace a správa virtuálních kontrolerů a virtuálních domén;
- diagnostiku a testování storage zařízení, řešení nestandardních a chybových stavů;
- generování repotů využití kapacit a analýza vytíženosti storage zařízení.

VIII.SOUČINNOST PRO ZAJIŠTĚNÍ POSKYTOVÁNÍ SLUŽBY

- Objednatel stanoví seznam určených osob pro přístup do prostředí nástroje SIEM, tento seznam předá Poskytovateli do 5 pracovních dnů od účinnosti zahájení Služby bezpečnostního monitoringu. Objednatel je povinen každou změnu určených osob prokazatelně oznámit Poskytovateli.
- Objednatel stanoví Poskytovateli kontaktní osoby včetně komunikační matice pro případ řešení kybernetických bezpečnostních událostí a incidentů (např. CSIRT tým Objednatele).
- V případě, že Objednatel využívá třetí strany pro správu, servis, podporu, konfiguraci apod. systému/ů monitorovaného/ných v rámci Služby, bude pro zjištění nebo řešení KBU/KBI zajištěna komunikační matice pro přímou komunikaci mezi Poskytovatelem a touto třetí stranou, a to obousměrně. Komunikace bude na straně Poskytovatele zaznamenána a evidována v tiketech v systému Service Desk Poskytovatele. Objednatel bude o této komunikaci dostávat notifikace. Komunikace mezi třetí stranou a Poskytovatelem bude v režimu 24/7. V případě, že třetí strana zjistí KBU/KBI, bude primárně kontaktovat Service Desk Poskytovatele.
- Objednatel poskytne nezbytnou součinnost Poskytovateli při vytváření výstupů Služby při nominacích kompetentních osob poskytujících součinnost při zpracování výstupů Služby na straně Objednatele a jeho smluvních partnerů. Zejména se jedná o nominace bezpečnostních rolí do realizačních týmů a stanovení jejich potřebných odpovědností a kompetencí s ohledem na poskytovanou Službu;
- Objednatel poskytne nezbytnou součinnost Poskytovateli při zajištění potřebné disponibility nominovaných členů realizačních týmů pro poskytnutí součinnosti s ohledem na odsouhlasené termíny;
- Objednatel poskytne nezbytnou součinnost pro zajištění řádného poskytování služeb Poskytovatelem dle tohoto katalogového listu (e.g. virtualizační prostředky).
- Objednatel poskytne dokumentaci logů, jejich významu, významu polí a use-case pro spouštění incident response, zejména k aplikacím
- Hlášení poruchy Služby oznamuje Objednatel na Service Desk Poskytovatele.

IX.PRINCIP STANOVENÍ CENY

Cena bude stanovena na základě požadavku Objednatele a za využití relevantní dokumentace zpracované Poskytovatelem, a to formou a za podmínek Vstupní analýzy pro následné poskytování Služby KL002.

V rámci Vstupní analýza bude stanoveno množství jednotek pro zajištění řádného poskytování Služby KL002. Výsledná cena Služby KL002 se stanoví v souladu s ujednáním dle čl. V odst. 5.1 pododst. 5.1.2. Smlouvy.

Vstupní analýza bude zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování odpovídajícího plnění.

Realizace Vstupní analýzy je povinným vstupem pro řádné stanovení ceny Služby KL002, kdy je rozhodné naplnění zpracování dílčího plnění dle výše zmíněné Rámcové smlouvy, a to:

- zpracování dokumentu „Závěrečná zpráva analýzy řešení bezpečnostního monitoringu v rozsahu informačního systému Objednatele".

Realizace ověření provozu bude zpracovaná Poskytovatelem a předaná Objednateli v rámci poskytování odpovídajícího plnění.

Vstupem a povinnou podmínkou pro Realizaci ověření provozu je dokument „Závěrečná zpráva analýzy řešení bezpečnostního monitoringu v rozsahu informačního systému Objednatele" zpracovaný dle Vstupní analýzy, dle kapitoly 3.1.

Realizace ověření provozu je povinným vstupem pro řádné stanovení ceny Služby KL002.

Služba Vstupní analýza a Realizace ověření provozu není samostatným Výstupem plnění Služby KL002 dle kapitoly 3.2.

X.POUŽITÉ VÝRAZY

Výraz	Popis
SPCSS	Státní pokladna Centrum sdílených služeb, s. p.
SPCSS NDC	Datové centrum SPCSS ve smyslu NDC i DCZ.
OCKB – SPCSS	Odbor Centra Kybernetické Bezpečnosti ve společnosti SPCSS.
Computer Security Incident Response Team (CSIRT–SPCSS)	Bezpečnostní tým ve společnosti SPCSS – zajišťuje spolupráci při řešení bezpečnostních incidentů. Na rozdíl od běžného bezpečnostního týmu je CSIRT zapojen do národní a světové bezpečnostní infrastruktury, která umožňuje sdílení informací a stanovení formálních postupů.
Security Operations Center (SOC)	Označuje specializované pracoviště v SPCSS, které soustřeďuje složky ochrany informačních dat a systémů. Toto pracoviště využívá k ochraně bezpečnosti celou řadu softwarových a hardwarových systémů, obsahuje celou řadu automatických nástrojů, pro odhalení útoků, které by člověk mohl přehlédnout. Cíl SOC: • Monitorování a ochrana před pokusy o průnik do systémů. • Zajištění souladu činností s právními předpisy, jež se týkají ochrany dat.
Kritická informační infrastruktura (KII)	KII je prvek nebo systém prvků kritické infrastruktury. Narušení jeho funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.
Významný informační systém (VIS)	VIS je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.
ZoKB	Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
Významná síť	Je síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.
CSIRT	Computer Security Incident Response Team. Základní povinností každého CSIRT týmu je spolupráce při řešení incidentů („response“).
BH	Bezpečnostní hlášení – jedná se o hlášení zadané do aplikace Service Desk přímo koncovým uživatelem, který má podezření na KBU nebo KBI.
KBU	Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
KBI	Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. • Kategorie III – velmi významný kybernetický bezpečnostní incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod, • Kategorie II – významný kybernetický bezpečnostní incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno

Výraz	Popis
	dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod, nebo • Kategorie I – méně významný kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.
SIEM	Security information and event management se zabývá dlouhodobým ukládáním událostí, jejich analýzou a hlášením problémů.
Offense	Přestupek, porušení pravidel, narušení systému, které detekoval nástroj SIEM.
Intrusion Detection Systems (IDS) Intrusion Prevention Systems (IPS)	Jedná se o systémy, které jsou schopny rozpoznat škodlivé aktivity v síti, zaznamenávat informace spojené s touto aktivitou. K detekci používají sledování anomálií ve využívání síťových protokolů a sledování anomálií provozu jako takového. Hlavní vlastností IPS a IDS je detekce podezřelého chování pomocí signatur. Systém IPS umí vzniklý nebezpečný provoz blokovat, IDS škodlivé chování pouze detekuje.
User behavior analytics (UBA)	Uživatelská behaviorální analýza – využívá zkoumání chování uživatele bez předchozí znalosti osobnosti. Systém vytváří vlastní vzorek každého uživatele a vyhodnocuje změny, které se odklání od obvyklého chování. *Např. uživatel provádí aktivitu v takové míře nebo z místa, které neodpovídá předchozímu chování. Naprostá pravidelnost a rychlost, která provází podezřelou činnost, může nasvědčovat, že došlo k odcizení identity a aktivitu provádí škodlivá aplikace, nikoliv člověk.*
Forenzní analýza	Prostředek, který pomáhá při řešení bezpečnostních incidentů slouží pro získání důkazů.
NetFlow	Otevřený protokol vyvinutý společností Cisco Systems. Poskytuje informace z třetí a čtvrté vrstvy referenčního modelu ISO/OSI.
NetFlow exportér	Směrovač, přepínač, speciální sonda. Zařízení, které je připojeno k monitorované lince a analyzuje procházející pakety. Na základě zachycených IP toků generuje NetFlow statistiky a ty exportuje na NetFlow kolektor. • Využití směrovačů – sledování a zpracování NetFlow informací má vliv na výkon zařízení. • Speciální sondy – specializované zařízení neviditelné v síti (instalované do L2), které nezasahuje do provozu. Statistiky jsou obvykle předávány dedikovaným rozhraním.
NetFlow kolektor	NetFlow kolektor je zařízení s velkou úložnou kapacitou, které sbírá statistiky z většího počtu NetFlow exportérů a ukládá je do dlouhodobé databáze.
Informace typu PCI	Payment Card Industry – informace o platebních kartách.
Informace typu PII, SPI	PII – Personally identifying information – osobní informace. SPI – Sensitive personal information – citlivé osobní informace.
Honey pots	Jedná se o „návnadný" systém, který je určen k detekci pokusů neoprávněného použití systémů a detekce podezřelého chování. Systém se tváří jako legitimní systém pro přilákání pozornosti případného útočníka. Všechny aktivity jsou monitorovány.
Podpora L1	První úroveň technické podpory poskytované Poskytovatelem.
Jednotka bezpečnostního monitoringu	Jedná se o hodnotu, která uvádí, kolik událostí dokáže generovat sledovaný systém nebo aplikace během jedné sekundy. Hodnota se může měnit dle zátěže, stavu systému nebo aplikace.

ZÁZNAM O POSKYTNUTÍ SLUŽEB

dle Smlouvy o poskytování služeb (evid. u Poskytovatele pod č. SML2024115 a u Objednatele pod 9166/2024-NBÚ/80)

Vykazované období:	od	do

Obě Smluvní strany potvrzují, že v uvedeném období byly v souladu s výše uvedenou Smlouvou poskytnuty níže specifikované Služby v účtovaném množství:

Oblast Služeb	**Celková cena za oblast Služby v období (Kč)**		
	bez DPH	**DPH**	**s DPH**
Služba infrastruktury PaaS			
Služba Bezpečnostní monitoring – ověřovací provoz			
Služba Bezpečnostní monitoring			
Celkem			

Za Objednatele	Za Poskytovatele
Datum:	Datum:
Jméno, příjmení Oprávněné osoby Objednatele:	Jméno, příjmení Oprávněné osoby Poskytovatele:
Podpis:	Podpis:

Státní pokladna Centrum sdílených služeb, s. p.

se sídlem Na Vápence 915/14, Žižkov, 130 00 Praha 3

ZPRÁVA

o úrovni a rozsahu poskytovaných Služeb v období

_____ - _____

dle Smlouvy o poskytování služeb
(evid. u Poskytovatele pod č. SML2024115 a u Objednatele 9166/2024-NBÚ/80)

Vypracoval		Schválil	
Jméno a příjmení:		Jméno a příjmení:	
Podpis		Podpis	
Datum:		Datum:	
Vyjádření Objednatele k poskytování Služeb:			
Za Objednatele			
Jméno a příjmení:			
Podpis			
Datum:			

AKCEPTAČNÍ PROTOKOL

Předmět	*[BUDE DOPLNĚNO]*		
Rámcová smlouva *(dále jen „**Rámcová smlouva**")*	*[BUDE DOPLNĚNO]*		
Objednatel *(dále jen „**Objednatel**")*	*[BUDE DOPLNĚNO]*		
Poskytovatel *(dále jen „**Poskytovatel**")*	*[BUDE DOPLNĚNO]*		
Vypracoval	*[BUDE DOPLNĚNO]*	***Datum***	*[BUDE DOPLNĚNO]*

Předmět akceptace
[BUDE DOPLNĚNO]

Připomínky Objednatele
[BUDE DOPLNĚNO]

Závěry akceptace	
☐	*je akceptováno bez výhrad*
☐	*je akceptováno s výhradou*
☐	*není akceptováno*

Seznam výhrad akceptace

P. č.	***Popis výhrady***	***Způsob odstranění***	***Termín odstranění***	***Zodpovědná osoba***
1	*[BUDE DOPLNĚNO]*	*[BUDE DOPLNĚNO]*	*[BUDE DOPLNĚNO]*	*[BUDE DOPLNĚNO]*

Seznam příloh akceptace

P. č.	***Název přílohy***
1	*[BUDE DOPLNĚNO]*
2	*[BUDE DOPLNĚNO]*

Schvalovací doložka

Jméno a příjmení	***Organizace***	***Datum a podpis***
[BUDE DOPLNĚNO]	*Objednatel*	*[elektronický podpis včetně data podpisu]*
[BUDE DOPLNĚNO]	*Poskytovatel*	*[elektronický podpis včetně data podpisu]*